



# Welcome to CCSP (Certified Cloud Security Professional)

Kelly Handerhan, Instructor

**VOLUME 2**



# Welcome!

- Your Instructor, Kelly Handerhan
- KellyH@CyberTrain.IT
- Over twenty years experience in Information Systems, Information Assurance, and Cybersecurity
- CCSP, CISSP, CASP, Security+, PMP, CRISC, CISM
- One of the original instructors for Cybrary.it
- Owner and lead technical instructor and instructional designer for www.CyberTrain.IT





Certified Cloud  
Security Professional

---

## Certification **Exam Outline**





# About CCSP

(ISC)<sup>2</sup> and the Cloud Security Alliance (CSA) developed the Certified Cloud Security Professional (CCSP) credential to ensure that cloud security professionals have the required knowledge, skills, and abilities in cloud security design, implementation, architecture, operations, controls, and compliance with regulatory frameworks. A CCSP applies information security expertise to a cloud computing environment and demonstrates competence in cloud security architecture, design, operations, and service orchestration. This professional competence is measured against a globally recognized body of knowledge. The CCSP is a stand-alone credential that complements and builds upon existing credentials and educational programs, including (ISC)<sup>2</sup>'s Certified Information Systems Security Professional (CISSP) and CSA's Certificate of Cloud Security Knowledge (CCSK).

The topics included in the CCSP Common Body of Knowledge (CBK) ensure its relevancy across all disciplines in the field of cloud security. Successful candidates are competent in the following 6 domains:

- Architectural Concepts & Design Requirements
- Cloud Data Security
- Cloud Platform & Infrastructure Security
- Cloud Application Security
- Operations
- Legal & Compliance

## Experience Requirements

Candidates must have a minimum of 5 years cumulative paid full-time work experience in information technology, of which 3 years must be in information security and 1 year in 1 or more of the 6 domains of the CCSP CBK. Earning CSA's CCSK certificate can be substituted for 1 year of experience in 1 or more of the 6 domains of the CCSP CBK. Earning (ISC)<sup>2</sup>'s CISSP credential can be substituted for the entire CCSP experience requirement.

A candidate that doesn't have the required experience to become a CCSP may become an Associate of (ISC)<sup>2</sup> by successfully passing the CCSP examination. The Associate of (ISC)<sup>2</sup> will then have 6 years to earn the 5 years required experience.

## Accreditation

CCSP under ANSI review for compliance with the stringent requirements of ANSI/ISO/IEC Standard 17024.

## Job Task Analysis (JTA)

(ISC)<sup>2</sup> has an obligation to its membership to maintain the relevancy of the CCSP. Conducted at regular intervals, the Job Task Analysis (JTA) is a methodical and critical process of determining the tasks that are performed by security professionals who are engaged in the profession defined by the CCSP. The results of the JTA are used to update the examination. This process ensures that candidates are tested on the topic areas relevant to the roles and responsibilities of today's practicing information security professionals focusing on cloud technologies.



## CCSP Examination Information

<b>Length of exam</b>	4 hours
<b>Number of questions</b>	125
<b>Question format</b>	Multiple choice
<b>Passing grade</b>	700 out of 1000 points
<b>Exam availability</b>	English
<b>Testing center</b>	Pearson VUE Testing Center

## CCSP Examination Weights

Domains	Weight
1. Architectural Concepts & Design Requirements	19%
2. Cloud Data Security	20%
3. Cloud Platform & Infrastructure Security	19%
4. Cloud Application Security	15%
5. Operations	15%
6. Legal & Compliance	12%
<b>Total: 100%</b>	



# Domain 1: Architectural Concepts and Design Requirements

## 1.1 Understand Cloud Computing Concepts

- » Cloud Computing Definitions (ISO/IEC 17788)
- » Cloud Computing Roles (i.e., Cloud Service Customer, Cloud Service Provider, and Cloud Service Partner)
- » Key Cloud Computing Characteristics (e.g., on-demand self-service, broad network access, multi-tenancy, rapid elasticity and scalability, resource pooling, measured service)
- » Building Block Technologies (e.g., virtualization, storage, networking, databases)

## 1.2 Describe Cloud Reference Architecture

- » Cloud Computing Activities (ISO/IEC 17789, Clause 9)
- » Cloud Service Capabilities (i.e., application capability type, platform capability type, infrastructure capability types)
- » Cloud Service Categories (e.g., SaaS, IaaS, PaaS, NaaS, CompaaS, DSaaS)
- » Cloud Deployment Models (e.g., public, private, hybrid, community)
- » Cloud Cross-Cutting Aspects (e.g., interoperability, portability, reversibility, availability, security, privacy, resiliency, performance, governance, maintenance and versioning, service levels and service level agreement, auditability, and regulatory)

## 1.3 Understand Security Concepts Relevant to Cloud Computing

- » Cryptography (e.g. encryption, in motion, at rest, key management)
- » Access Control
- » Data and Media Sanitization (e.g., overwriting, cryptographic erase)
- » Network security
- » Virtualization Security (e.g., hypervisor security)
- » Common Threats
- » Security Considerations for different Cloud Categories (e.g., SaaS, PaaS, \*aaS)

## 1.4 Understand Design Principles of Secure Cloud Computing

- » Cloud Secure Data Lifecycle
- » Cloud Based Business Continuity/Disaster Recovery Planning
- » Cost Benefit Analysis
- » Functional Security Requirements (e.g., portability, interoperability, vendor lock-in)

## 1.5 Identify Trusted Cloud Services

- » Certification Against Criteria
- » System/Subsystem Product Certifications (e.g., common criteria, FIPS 140-2)



## Domain 2: Cloud Data Security

### 2.1 Understand Cloud Data Lifecycle (CSA Guidance)

- » Phases
- » Relevant Data Security Technologies

### 2.2 Design and Implement Cloud Data Storage Architectures

- » Storage Types (e.g. long term, ephemeral, raw-disk)
- » Threats to Storage Types (e.g., ISO/IEC 27040)
- » Technologies Available to Address Threats (e.g., encryption)

### 2.3 Design and Apply Data Security Strategies

- » Encryption
- » Key Management
- » Masking
- » Tokenization
- » Application of Technologies (e.g., time of storage vs. encryption needs)
- » Emerging Technologies (e.g., bit splitting, data obfuscation, homomorphic encryption)

### 2.4 Understand and Implement Data Discovery and Classification Technologies

- » Data Discovery
- » Classification

### 2.5 Design and Implement Relevant Jurisdictional Data Protections for Personally Identifiable Information (PII)

- » Data Privacy Acts
- » Implementation of Data Discovery
- » Classification of Discovered Sensitive Data
- » Mapping and Definition of Controls
- » Application of Defined Controls for PII (in consideration of customer's Data Privacy Acts)

### 2.6 Design and Implement Data Rights Management

- » Data Rights Objectives (e.g. provisioning, users and roles, role-based access)
- » Appropriate Tools (e.g., Issuing and replication of certificates)



## 2.7 Plan and Implement Data Retention, Deletion, and Archiving Policies

- » Data Retention Policies
- » Data Deletion Procedures and Mechanisms
- » Data Archiving Procedures and Mechanisms

## 2.8 Design and Implement Auditability, Traceability and Accountability of Data Events

- » Definition of Event Sources and Identity Attribution Requirement
- » Data Event Logging
- » Storage and Analysis of Data Events (e.g. security information and event management)
- » Continuous Optimizations (e.g. new events detected, add new rules, reductions of false positives)
- » Chain of Custody and Non-repudiation



## Domain 3: Cloud Platform and Infrastructure Security

### 3.1 Comprehend Cloud Infrastructure Components

- » Physical Environment
- » Network and Communications
- » Compute
- » Virtualization
- » Storage
- » Management Plane

### 3.2 Analyze Risks Associated to Cloud Infrastructure

- » Risk Assessment/Analysis
- » Cloud Attack Vectors
- » Virtualization Risks
- » Counter-Measure Strategies (e.g., access controls, design principles)

### 3.3 Design and Plan Security Controls

- » Physical and Environmental Protection (e.g., on-premise)
- » System and Communication Protection
- » Virtualization Systems Protection
- » Management of Identification, Authentication and Authorization in Cloud Infrastructure
- » Audit Mechanisms

### 3.4 Plan Disaster Recovery and Business Continuity Management

- » Understanding of the Cloud Environment
- » Understanding of the Business Requirements
- » Understanding of the Risks
- » Disaster Recovery/Business Continuity strategy
- » Creation of the Plan
- » Implementation of the Plan



## Domain 4: Cloud Application Security

### 4.1 Recognize the need for Training and Awareness in Application Security

- » Cloud Development Basics (e.g., RESTful)
- » Common Pitfalls
- » Common Vulnerabilities (e.g. OWASP Top 10)

### 4.2 Understand Cloud Software Assurance and Validation

- » Cloud-based Functional Testing
- » Cloud Secure Development Lifecycle
- » Security Testing (e.g., SAST, DAST, Pen Testing)

### 4.3 Use Verified Secure Software

- » Approved API
- » Supply-Chain Management
- » Community Knowledge

### 4.4 Comprehend the Software Development Life-Cycle (SDLC) Process

- » Phases & Methodologies
- » Business Requirements
- » Software Configuration Management & Versioning

### 4.5 Apply the Secure Software Development Life-Cycle

- » Common Vulnerabilities (e.g., SQL Injection, XSS, XSRF, Direct Object Reference, Buffer Overflow)
- » Cloud-Specific Risks
- » Quality of Service
- » Threat Modeling



#### 4.6 Comprehend the Specifics of Cloud Application Architecture

- » Supplemental Security Devices (e.g., WAF, DAM, XML firewalls, API gateway)
- » Cryptography (e.g. TLS, SSL, IPSEC)
- » Sandboxing
- » Application Virtualization

#### 4.7 Design Appropriate Identity and Access Management (IAM) Solutions

- » Federated Identity
- » Identity Providers
- » Single Sign-On
- » Multi-factor Authentication



## Domain 5: Operations

### 5.1 Support the Planning Process for the Data Center Design

- » Logical Design (e.g., tenant partitioning, access control)
- » Physical Design (e.g., location, buy or build)
- » Environmental Design (e.g., HVAC, multi-vendor pathway connectivity)

### 5.2 Implement and Build Physical Infrastructure for Cloud Environment

- » Secure Configuration of Hardware Specific Requirements (e.g., BIOS settings for virtualization and TPM, storage controllers, network controllers)
- » Installation and Configuration of Virtualization Management Tools for the Host

### 5.3 Run Physical Infrastructure for Cloud Environment

- » Configuration of Access Control for Local Access (e.g., Secure KVM, Console based access mechanisms)
- » Securing Network Configuration (e.g., VLAN's, TLS, DHCP, DNS, IPSEC)
- » OS Hardening via Application of Baseline (e.g., Windows, Linux, VMware)
- » Availability of Stand-Alone Hosts
- » Availability of Clustered Hosts (e.g., distributed resource scheduling (DRS), dynamic optimization (DO), storage clusters, maintenance mode, high availability)

### 5.4 Manage Physical Infrastructure for Cloud Environment

- » Configuring Access Controls for Remote Access (e.g., RDP, Secure Terminal Access)
- » OS Baseline Compliance Monitoring and Remediation
- » Patch Management
- » Performance Monitoring (e.g., network, disk, memory, CPU)
- » Hardware Monitoring (e.g., disk I/O, CPU temperature, fan speed)
- » Backup and Restore of Host Configuration
- » Implementation of Network Security Controls (e.g., firewalls, IDS, IPS, honeypots, vulnerability assessments)
- » Log Capture and Analysis (e.g., SIEM, Log Management)
- » Management Plane (e.g., scheduling, orchestration, maintenance)



## 5.5 Build Logical Infrastructure for Cloud Environment

- » Secure Configuration of Virtual Hardware Specific Requirements (e.g., network, storage, memory, CPU)
- » Installation of Guest O/S Virtualization Toolsets

## 5.6 Run Logical Infrastructure for Cloud Environment

- » Secure Network Configuration (e.g., VLAN's, TLS, DHCP, DNS, IPSEC)
- » OS Hardening via Application of a Baseline (e.g., Windows, Linux, VMware)
- » Availability of the Guest OS

## 5.7 Manage Logical Infrastructure for Cloud Environment

- » Access Control for Remote Access (e.g., RDP)
- » OS Baseline Compliance Monitoring and Remediation
- » Patch Management
- » Performance Monitoring (e.g., Network, Disk, Memory, CPU)
- » Backup and Restore of Guest OS Configuration (e.g., Agent based, SnapShots, Agentless)
- » Implementation of Network Security Controls (e.g., firewalls, IDS, IPS, honeypots, vulnerability assessments)
- » Log Capture and Analysis (e.g., SIEM, log management)
- » Management Plane (e.g., scheduling, orchestration, maintenance)

## 5.8 Ensure Compliance with Regulations and Controls (e.g., ITIL, ISO/IEC 20000-1)

- » Change Management
- » Continuity Management
- » Information Security Management
- » Continual Service Improvement Management
- » Incident Management
- » Problem Management
- » Release Management
- » Deployment Management
- » Configuration Management
- » Service Level Management
- » Availability Management
- » Capacity Management

## 5.9 Conduct Risk Assessment to Logical and Physical Infrastructure



## 5.10 Understand the Collection, Acquisition and Preservation of Digital Evidence

- » Proper Methodologies for Forensic Collection of Data
- » Evidence Management

## 5.11 Manage Communication with Relevant Parties

- » Vendors
- » Customers
- » Partners
- » Regulators
- » Other Stakeholders



## Domain 6: Legal and Compliance

### 6.1 Understand Legal Requirements and Unique Risks within the Cloud Environment

- » International Legislation Conflicts
- » Appraisal of Legal Risks Specific to Cloud Computing
- » Legal Controls
- » eDiscovery (e.g., ISO/IEC 27050, CSA Guidance)
- » Forensics Requirements

### 6.2 Understand Privacy Issues, Including Jurisdictional Variation

- » Difference between Contractual and Regulated PII
- » Country-Specific Legislation Related to PII / Data Privacy
- » Difference Among Confidentiality, Integrity, Availability, and Privacy

### 6.3 Understand Audit Process, Methodologies, and Required Adaptations for a Cloud Environment

- » Internal and External Audit Controls
- » Impact of Requirements Programs by the Use of Cloud
- » Assurance Challenges of Virtualization and Cloud
- » Types of Audit Reports (e.g., SAS, SSAE, ISAE)
- » Restrictions of Audit Scope Statements (e.g., SAS 70)
- » Gap Analysis
- » Audit Plan
- » Standards Requirements (e.g., ISO/IEC 27018, GAPP)
- » Internal Information Security Management System
- » Internal information Security Controls System
- » Policies
- » Identification and Involvement of Relevant Stakeholders
- » Specialized Compliance Requirements for Highly Regulated Industries
- » Impact of Distributed IT Model (e.g., diverse geographical locations and crossing over legal jurisdictions)



## 6.4 Understand Implications of Cloud to Enterprise Risk Management

- » Access Providers Risk Management
- » Difference between Data Owner/Controller vs. Data Custodian/Processor (e.g., risk profile, risk appetite, responsibility)
- » Provision of Regulatory Transparency Requirements
- » Risk Mitigation
- » Different Risk Frameworks
- » Metrics for Risk Management
- » Assessment of Risk Environment (e.g., service, vendor, ecosystem)

## 6.5 Understand Outsourcing and Cloud Contract Design

- » Business Requirements (e.g., SLA, GAAP)
- » Vendor Management (e.g., selection, common certification framework)
- » Contract Management (e.g., right to audit, metrics, definitions, termination, litigation, assurance, compliance, access to cloud/data)

## 6.6 Execute Vendor Management

- » Supply-chain Management (e.g., ISO/IEC 27036)



# Additional Examination Information

## Supplementary References

Candidates are encouraged to supplement their education and experience by reviewing relevant resources that pertain to the CBK and identifying areas of study that may need additional attention.

View the full list of supplementary references at [www.isc2.org/ccsp-cbk-references](http://www.isc2.org/ccsp-cbk-references).

## Examination Policies and Procedures

(ISC)<sup>2</sup> recommends that CCSP candidates review exam policies and procedures prior to registering for the examination. Read the comprehensive breakdown of this important information at [www.isc2.org/exam-policies-procedures](http://www.isc2.org/exam-policies-procedures).

## Legal Info

For any questions related to (ISC)<sup>2</sup>'s legal policies, please contact the (ISC)<sup>2</sup> Legal Department at [legal@isc2.org](mailto:legal@isc2.org).

## Any Questions?

(ISC)<sup>2</sup> Candidate Services  
311 Park Place Blvd, Suite 400  
Clearwater, FL 33759

(ISC)<sup>2</sup> Americas  
Tel: +1.727.785.0189  
Email: [info@isc2.org](mailto:info@isc2.org)

(ISC)<sup>2</sup> Asia Pacific  
Tel: +(852) 28506951  
Email: [isc2asia@isc2.org](mailto:isc2asia@isc2.org)

(ISC)<sup>2</sup> EMEA  
Tel: +44 (0)203 300 1625  
Email: [info-emea@isc2.org](mailto:info-emea@isc2.org)



# SECURITY GUIDANCE

---

For Critical Areas of Focus  
In Cloud Computing v4.0



The permanent and official location for Cloud Security Alliance's *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0* is <https://cloudsecurityalliance.org/download/security-guidance-v4/>.



© 2017 Cloud Security Alliance – All Rights Reserved.

The Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 ("Guidance v4.0") is licensed by the Cloud Security Alliance under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC-BY-NC-SA 4.0).

*Sharing* - You may share and redistribute the Guidance in any medium or any format, only for non-commercial purposes.

*Adaptation* - You may adapt, transform, modify and build upon the Guidance v4 and distribute the modified Guidance v4.0, only for non-commercial purposes.

*Attribution* - You must give credit to the Cloud Security Alliance, link to Guidance v4.0 webpage located at <https://cloudsecurityalliance.org/download/security-guidance-v4/>, and indicate whether changes were made. You may not suggest that CSA endorsed you or your use.

*Share-Alike* - All modifications and adaptations must be distributed under the same license as the original Guidance v4.0.

*No additional restrictions* - You may not apply legal terms or technological measures that restrict others from doing anything that this license permits.

*Commercial Licenses* - If you wish to adapt, modify, share or distribute copies of the Guidance v4.0 for revenue generating purposes you must first obtain an appropriate license from the Cloud Security Alliance. Please contact us at [info@cloudsecurityalliance.org](mailto:info@cloudsecurityalliance.org).

Notices: All trademark, copyright or other notices affixed onto the Guidance v4.0 must be reproduced and may not be removed.

# FOREWORD

Welcome to the fourth version of the Cloud Security Alliance's *Security Guidance for Critical Areas of Focus in Cloud Computing*. The rise of cloud computing as an ever-evolving technology brings with it a number of opportunities and challenges. With this document, we aim to provide both guidance and inspiration to support business goals while managing and mitigating the risks associated with the adoption of cloud computing technology.

The Cloud Security Alliance promotes implementing best practices for providing security assurance within the domain of cloud computing and has delivered a practical, actionable roadmap for organizations seeking to adopt the cloud paradigm. The fourth version of the *Security Guidance for Critical Areas of Focus in Cloud Computing* is built on previous iterations of the security guidance, dedicated research, and public participation from the Cloud Security Alliance members, working groups, and the industry experts within our community. This version incorporates advances in cloud, security, and supporting technologies; reflects on real-world cloud security practices; integrates the latest Cloud Security Alliance research projects; and offers guidance for related technologies.

The advancement toward secure cloud computing requires active participation from a broad set of globally-distributed stakeholders. CSA brings together this diverse community of industry partnerships, international chapters, working groups, and individuals. We are profoundly grateful to all who contributed to this release.

Please visit [cloudsecurityalliance.com](http://cloudsecurityalliance.com) to learn how you can work with us to identify and promote best practices to ensure a secure cloud computing environment.

Best regards,

**Luciano (J.R.) Santos**  
Executive Vice President of Research  
Cloud Security Alliance

# ACKNOWLEDGEMENTS

## Lead Authors

Rich Mogull  
James Arlen  
Francoise Gilbert  
Adrian Lane  
David Mortman  
Gunnar Peterson  
Mike Rothman

## Editors

John Moltz  
Dan Moren  
Evan Scoboria

## CSA Staff

Jim Reavis  
Luciano (J.R.) Santos  
Hillary Baron  
Ryan Bergsma  
Daniele Catteddu  
Victor Chin  
Frank Guanco  
Stephen Lumpe (Design)  
John Yeoh

## Contributors

On behalf of the CSA Board of Directors and the CSA Executive Team, we would like to thank all of the individuals who contributed time and feedback to this version of the CSA Security Guidance for Critical Areas of Focus in Cloud Computing. We value your volunteer contributions and believe that the devotion of volunteers like you will continue to lead the Cloud Security Alliance into the future.

# LETTER FROM THE CEO

I am thrilled by this latest contribution to the community's knowledge base of cloud security best practices that began with Cloud Security Alliance's initial guidance document released in April of 2009. We hope that you will carefully study the issues and recommendations outlined here, compare with your own experiences and provide us with your feedback. A big thank you goes out to all who participated in this research.

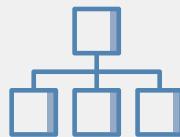
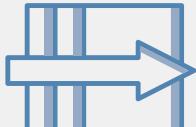
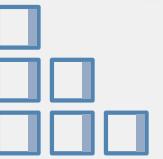
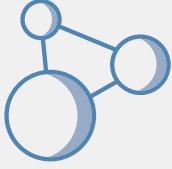
Recently, I had the opportunity to spend a day with one of the industry experts who helped found Cloud Security Alliance. He reflected that for the most part CSA has completed its initial mission, which was to prove that cloud computing could be made secure and to provide the necessary tools to that end. Not only did CSA help make cloud computing a credible secure option for information technology, but today cloud computing has become the default choice for IT and is remaking the modern business world in very profound ways.

The resounding success of cloud computing and CSA's role in leading the trusted cloud ecosystem brings with it even greater challenges and urgency into our renewed mission. Cloud is now becoming the back end for all forms of computing, including the ubiquitous Internet of Things. Cloud computing is the foundation for the information security industry. New ways of organizing compute, such as containerization and DevOps are inseparable from cloud and accelerating our revolution. At Cloud Security Alliance, we are committed to providing you the essential security knowledge you need for this fast moving IT landscape and staying at the forefront of next-generation assurance and trust trends. We welcome your participation in our community, always.

Best regards,

**Jim Reavis**  
Co-Founder & CEO  
Cloud Security Alliance

# TABLE OF CONTENTS

<b>DOMAIN 1</b> Cloud Computing Concepts and Architectures 	<b>DOMAIN 2</b> Governance and Enterprise Risk Management 	<b>DOMAIN 3</b> Legal Issues, Contracts and Electronic Discovery 	<b>DOMAIN 4</b> Compliance and Audit Management 
<b>DOMAIN 5</b> Information Governance 	<b>DOMAIN 6</b> Management Plane and Business Continuity 	<b>DOMAIN 7</b> Infrastructure Security 	<b>DOMAIN 8</b> Virtualization and Containers 
<b>DOMAIN 9</b> Incident Response 	<b>DOMAIN 10</b> Application Security 	<b>DOMAIN 11</b> Data Security and Encryption 	<b>DOMAIN 12</b> Identity, Entitlement, and Access Management 
<b>DOMAIN 13</b> Security as a Service 	<b>DOMAIN 14</b> Related Technologies 		



# DOMAIN 1

# Cloud Computing Concepts and Architectures

## 1.0 Introduction

This domain provides the conceptual framework for the rest of the Cloud Security Alliance's guidance. It describes and defines cloud computing, sets our baseline terminology, and details the overall logical and architectural frameworks used in the rest of the document.

There are many different ways of viewing cloud computing: It's a technology, a collection of technologies, an operational model, a business model, just to name a few. It is, at its essence, *transformative* and *disruptive*. It's also growing very, very quickly, and shows no signs of slowing down. While the reference models we included in the first version of this Guidance are still relatively accurate, they are most certainly no longer complete. And even this update can't possibly account for every possible evolution in the coming years.

Cloud computing offers tremendous potential benefits in *agility*, *resiliency*, and *economy*. Organizations can move faster (since they don't have to purchase and provision hardware, and everything is software defined), reduce downtime (thanks to inherent elasticity and other cloud characteristics), and save money (due to reduced capital expenses and better demand and capacity matching). We also see *security* benefits since cloud providers have significant economic incentives to protect customers.

However, these benefits only appear if you understand and adopt *cloud-native* models and adjust your architectures and controls to align with the features and capabilities of cloud platforms. In fact, taking an existing application or asset and simply moving it to a cloud provider without any changes will often reduce agility, resiliency, and even security, all while increasing costs.

The goal of this domain is to build the foundation that the rest of the document and its recommendations are based on. The intent is to provide a common language and understanding of cloud computing for security professionals, begin highlighting the differences between cloud and traditional computing, and help guide security professionals towards adopting cloud-native approaches that result in better security (and those other benefits), instead of creating more risks.

This domain includes 4 sections:

- Defining cloud computing
- The cloud logical model
- Cloud conceptual, architectural, and reference model
- Cloud security and compliance scope, responsibilities, and models

The Cloud Security Alliance isn't setting out to create an entirely new taxonomy or reference model. Our objective is to distill and harmonize existing models—most notably the work in [NIST Special Publication 800-145, ISO/IEC 17788 and ISO/IEC 17789](#)—and focus on what's most relevant to security professionals.

## 1.1 Overview

### 1.1.1 Defining Cloud Computing

Cloud computing is a new operational model and set of technologies for managing shared pools of computing resources.

It is a disruptive technology that has the potential to enhance collaboration, agility, scaling, and availability, as well as providing the opportunities for cost reduction through optimized and efficient computing. The cloud model envisages a world where components can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down to provide an on-demand utility-like model of allocation and consumption.

NIST defines cloud computing as:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The ISO/IEC definition is very similar:

Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

A (slightly) simpler way of describing cloud is that it takes a set of resources, such as processors and memory, and puts them into a big pool (in this case, using virtualization). Consumers ask for what they need out of the pool, such as 8 CPUs and 16 GB of memory, and the cloud assigns those resources to the client, who then connects to and uses them over the network. When the client is done, they can release the resources back into the pool for someone else to use.

A cloud can consist of nearly any computing resources, ranging from our “compute” examples of processors and memory to networks, storage, and higher level resources like databases and



applications. For example, subscribing to a customer-relations management application for 500 employees on a service shared by hundreds of other organizations is just as much cloud computing as launching 100 remote servers on a compute cloud.

Definition: A *cloud user* is the person or organization requesting and using the resources, and the *cloud provider* is the person or organization who delivers it. We also sometimes use the terms *client* and *consumer* to refer to the cloud user, and *service* or simply *cloud* to describe the provider. [NIST 500-292](#) uses the term “cloud actor” and adds roles for cloud brokers, carriers, and auditors. ISO/IEC 17788 uses the terms cloud service customer, cloud service partner, and cloud service provider.

The key techniques to create a cloud are abstraction and orchestration. We abstract the resources from the underlying physical infrastructure to create our pools, and use orchestration (and automation) to coordinate carving out and delivering a set of resources from the pools to the consumers. As you will see, these two techniques create all the essential characteristics we use to define something as a “cloud.”

This is the difference between cloud computing and traditional virtualization; virtualization abstracts resources, but it typically lacks the orchestration to pool them together and deliver them to customers on demand, instead relying on manual processes.

Clouds are *multitenant* by nature. Multiple different consumer constituencies share the same pool of resources but are *segregated* and *isolated* from each other. Segregation allows the cloud provider to divvy up resources to the different groups, and isolation ensures they can't see or modify each other's assets. Multitenancy doesn't only apply across different organizations; it's also used to divvy up resources between different units in a single business or organization.

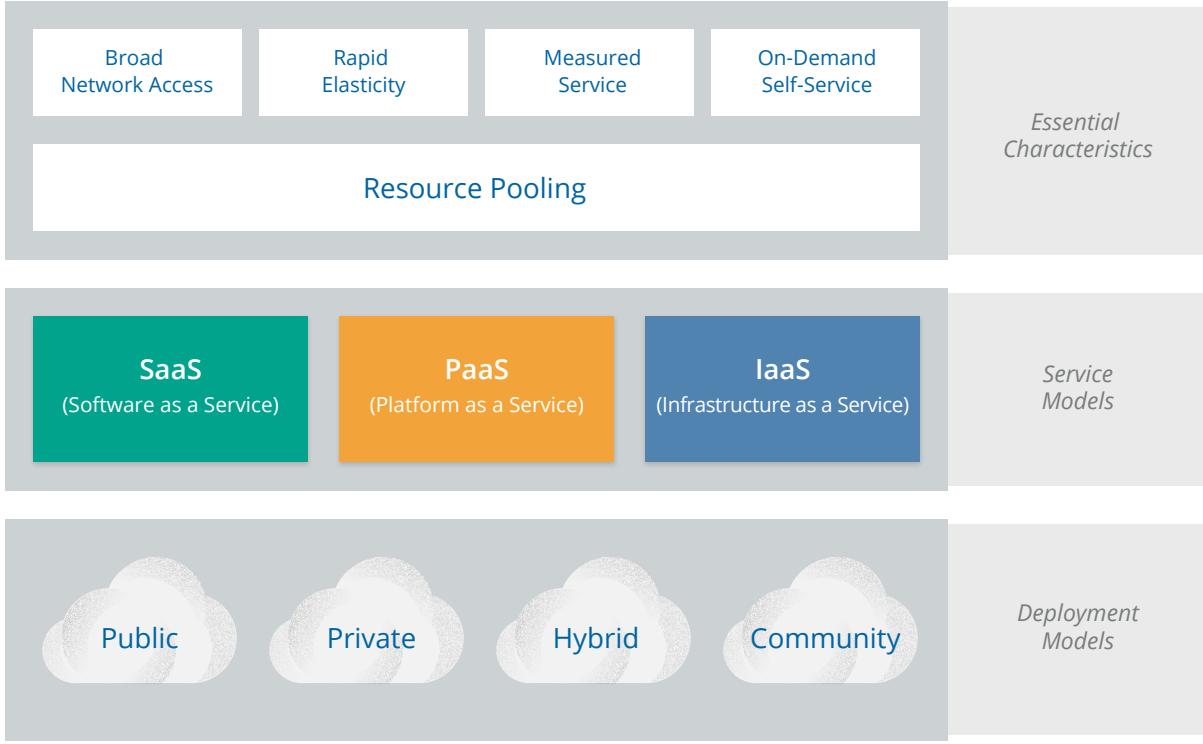
### **1.1.2 Definitional Model**

The Cloud Security Alliance (CSA) uses the [NIST model for cloud computing](#) as its standard for defining cloud computing. The CSA also endorses the [ISO/IEC model](#) which is more in-depth, and additionally serves as a reference model. Throughout this domain we will reference both.

NIST's publication is generally well accepted, and the Guidance aligns with the NIST Working Definition of Cloud Computing (NIST 800-145) to bring coherence and consensus around a common language to focus on use cases rather than semantic nuances.

It is important to note that this guide is intended to be broadly usable and applicable to organizations globally. While NIST is a U.S. government organization, the selection of this reference model should not be interpreted to suggest the exclusion of other points of view or geographies.

NIST defines cloud computing by describing five essential characteristics, three cloud service models, and four cloud deployment models. They are summarized in visual form and explained in detail on the following page.



### 1.1.2.1 Essential Characteristics

These are the characteristics that make a cloud a cloud. If something has these characteristics, we consider it cloud computing. If it lacks any of them, it is likely not a cloud.

- *Resource pooling* is the most fundamental characteristic, as discussed above. The provider abstracts resources and collects them into a pool, portions of which can be allocated to different consumers (typically based on policies).
- Consumers provision the resources from the pool using *on-demand self-service*. They manage their resources themselves, without having to talk to a human administrator.
- *Broad network access* means that all resources are available over a network, without any need for direct physical access; the network is not necessarily part of the service.
- *Rapid elasticity* allows consumers to expand or contract the resources they use from the pool (provisioning and deprovisioning), often completely automatically. This allows them to more closely match resource consumption with demand (for example, adding virtual servers as demand increases, then shutting them down when demand drops).
- *Measured service* meters what is provided, to ensure that consumers only use what they are allotted, and, if necessary, to charge them for it. This is where the term *utility computing* comes from, since computing resources can now be consumed like water and electricity, with the client only paying for what they use.

ISO/IEC 17788 lists six key characteristics, the first five of which are identical to the NIST characteristics. The only addition is *multitenancy*, which is distinct from resource pooling.



### 1.1.2.2 Service Models

NIST defines three *service models* which describe the different foundational categories of cloud services:

- *Software as a Service (SaaS)* is a full application that's managed and hosted by the provider. Consumers access it with a web browser, mobile app, or a lightweight client app.
- *Platform as a Service (PaaS)* abstracts and provides development or application platforms, such as databases, application platforms (e.g. a place to run Python, PHP, or other code), file storage and collaboration, or even proprietary application processing (such as machine learning, big data processing, or direct Application Programming Interfaces (API) access to features of a full SaaS application). The key differentiator is that, with PaaS, you don't manage the underlying servers, networks, or other infrastructure.
- *Infrastructure as a Service (IaaS)* offers access to a resource pool of fundamental computing infrastructure, such as compute, network, or storage.

We sometimes call these the "SPI" tiers.

ISO/IEC uses a more complex definition with a *cloud capabilities type* that maps closely to the SPI tiers (application, infrastructure, and platform capability types). It then expands into *cloud service categories* that are more granular, such as Compute as a Service, Data Storage as a Service, and then even includes IaaS/PaaS/SaaS.

These categories are somewhat permeable: Some cloud services span these tiers, others don't fall neatly into a single service model. Practically speaking, there's no reason to try and assign everything into these three broad categories, or even the more granular categories in the ISO/IEC model. This is merely a useful descriptive tool, not a rigid framework.

Both approaches are equally valid, but since the NIST model is more concise and currently used more broadly, it is the definition predominantly used in CSA research.

### 1.1.2.3 Deployment Models

Both NIST and ISO/IEC use the same four cloud deployment models. These are how the technologies are deployed and consumed, and they apply across the entire range of service models:

- *Public Cloud*. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- *Private Cloud*. The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or by a third party and may be located on-premises or off-premises.
- *Community Cloud*. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g. mission, security requirements, policy, or compliance considerations). It may be managed by the organizations or by a third party and may be located on-premises or off-premises.
- *Hybrid Cloud*. The cloud infrastructure is a composition of two or more clouds (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). Hybrid is also commonly used to describe a non-cloud data center bridged directly to a cloud provider.

Deployment models are defined based on the cloud user—that is, who uses the cloud. As the diagram below shows, the organization that owns and manages the cloud will vary even within a single deployment model.

	Infrastructure Owned By <sup>1</sup>	Infrastructure Owned By <sup>2</sup>	Infrastructure Located <sup>3</sup>	Accessible and Consumed By <sup>4</sup>
<b>Public</b>	Third-Party Provider	Third-Party Provider	Off-Premises	Untrusted
<b>Private/Community</b>	Organization Third-Party Provider	Organization Third-Party Provider	On-Premises Off-Premises	Trusted
<b>Hybrid</b>	Both Organization & Third-Party Provider	Both Organization & Third-Party Provider	Both On-Premises & Off-Premises	Trusted & Untrusted

<sup>1</sup> Management includes: governance, operations, security, compliance, etc...

<sup>2</sup> Infrastructure implies physical infrastructure such as facilities, compute network and storage equipment

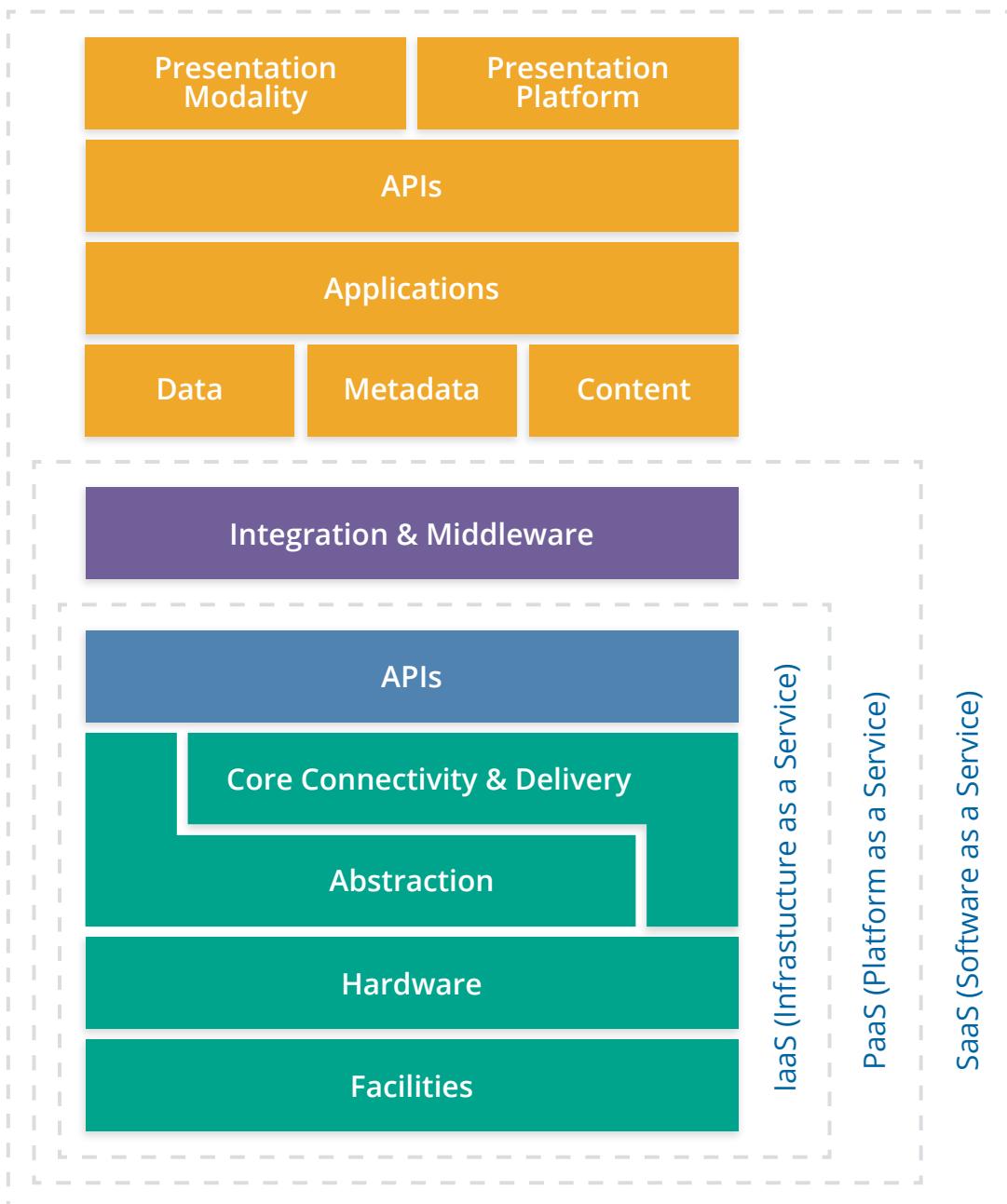
<sup>3</sup> Infrastructure location is both physical relative to an organization's management umbrella and speaks to ownership versus control

<sup>4</sup> Trusted consumers of service are those who are considered part of an organization's legal/contractual/policy umbrella including employees, contractors, and business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.

### 1.1.3 Reference and Architecture Models

These days there is a wide range of constantly evolving technological techniques for building cloud services, making any single reference or architectural model obsolete from the start. The objective of this section is to provide both some fundamentals to help security professionals make informed decisions as well as a baseline to understand more complex and emerging models. For an in-depth reference architectural model, we again recommend [ISO/IEC 17789](#) and [NIST 500-292](#), which complement the NIST definition model.

One way of looking at cloud computing is as a stack where Software as a Service is built on Platform as a Service, which is built on Infrastructure as a Service. This is not representative of all (or even most) real-world deployments, but serves as a useful reference to start the discussion.





### 1.1.3.1 Infrastructure as a Service

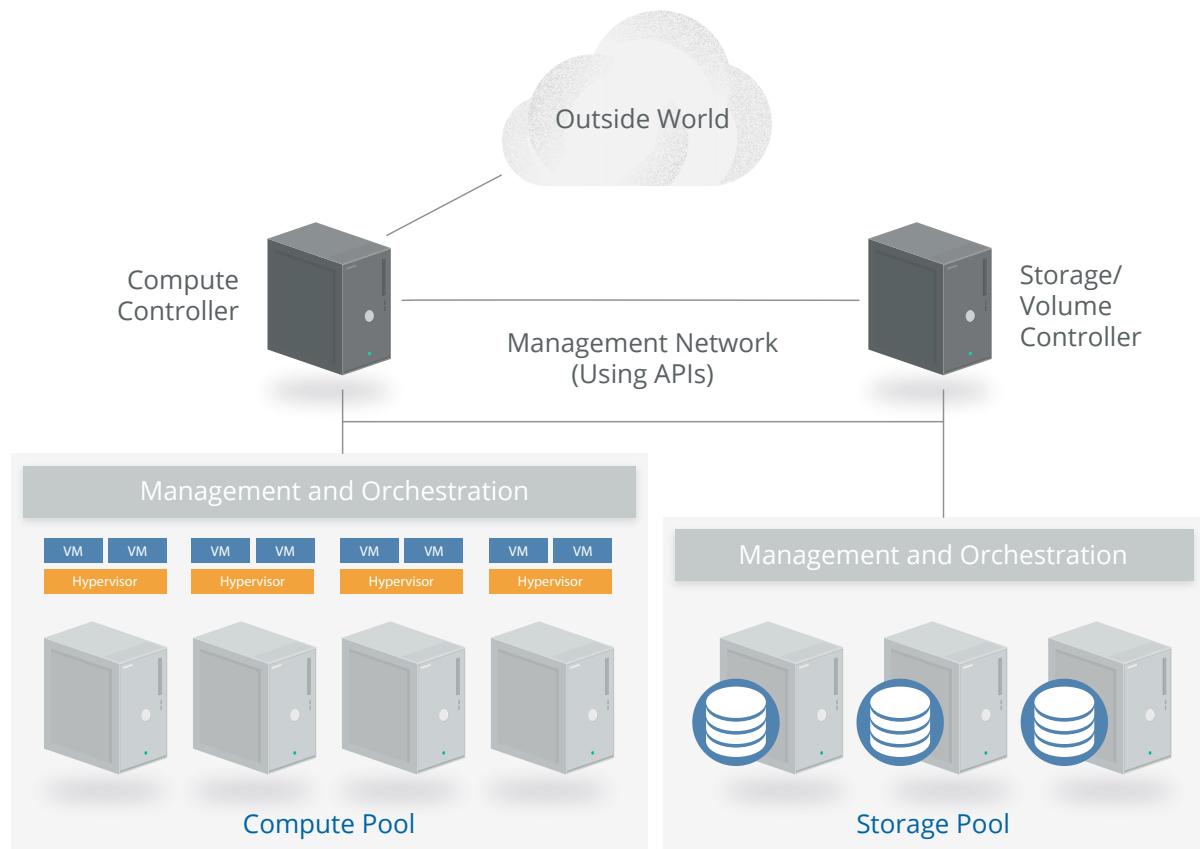
Physical facilities and infrastructure hardware form the foundation of IaaS. With cloud computing we abstract and pool these resources, but at the most basic level we always need physical hardware, networks, and storage to build on. These resources are pooled using abstraction and orchestration. Abstraction, often via virtualization, frees the resources from their physical constraints to enable pooling. Then a set of core connectivity and delivery tools (orchestration) ties these abstracted resources together, creates the pools, and provides the automation to deliver them to customers.

All this is facilitated using *Application Programming Interfaces*. APIs are typically the underlying communications method for components within a cloud, some of which (or an entirely different set) are exposed to the cloud user to manage their resources and configurations. Most cloud APIs these days use REST (Representational State Transfer), which runs over the HTTP protocol, making it extremely well suited for Internet services.

In most cases, those APIs are both remotely accessible and wrapped into a web-based user interface. This combination is the *cloud management plane*, since consumers use it to manage and configure the cloud resources, such as launching virtual machines (instances) or configuring virtual networks. From a security perspective, it is both the biggest difference from protecting physical infrastructure (since you can't rely on physical access as a control) and the top priority when designing a cloud security program. If an attacker gets into your management plane, they potentially have full remote access to your entire cloud deployment.

Thus IaaS consists of a facility, hardware, an abstraction layer, an orchestration (core connectivity and delivery) layer to tie together the abstracted resources, and APIs to remotely manage the resources and deliver them to consumers.

Here is a simplified architectural example of a compute IaaS platform:



*This is a very simple diagram showing the compute and storage controllers for orchestration, hypervisors for abstraction, and the relationship between the compute and storage pools. It omits many components, such as the network manager.*

A series of physical servers each run two components: a hypervisor (for virtualization) and the management/orchestration software to tie in the servers and connect them to the compute controller. A customer asks for an instance (virtual server) of a particular size and the cloud controller determines which server has the capacity and allocates an instance of the requested size.

The controller then creates a virtual hard drive by requesting storage from the storage controller, which allocates storage from the storage pool, and connects it to the appropriate host server and instance over the network (a dedicated network for storage traffic). Networking, including virtual network interfaces and addresses, is also allocated and connected to the necessary virtual network.

The controller then sends a copy of the server image into the virtual machine, boots it, and configures it; this creates an instance running in a virtual machine (VM), with virtual networking and storage all properly configured. Once this entire process is complete, the metadata and connectivity information is brokered by the cloud controller and available to the consumer, who can now connect to the instance and log in.



### 1.1.3.2 Platform as a Service

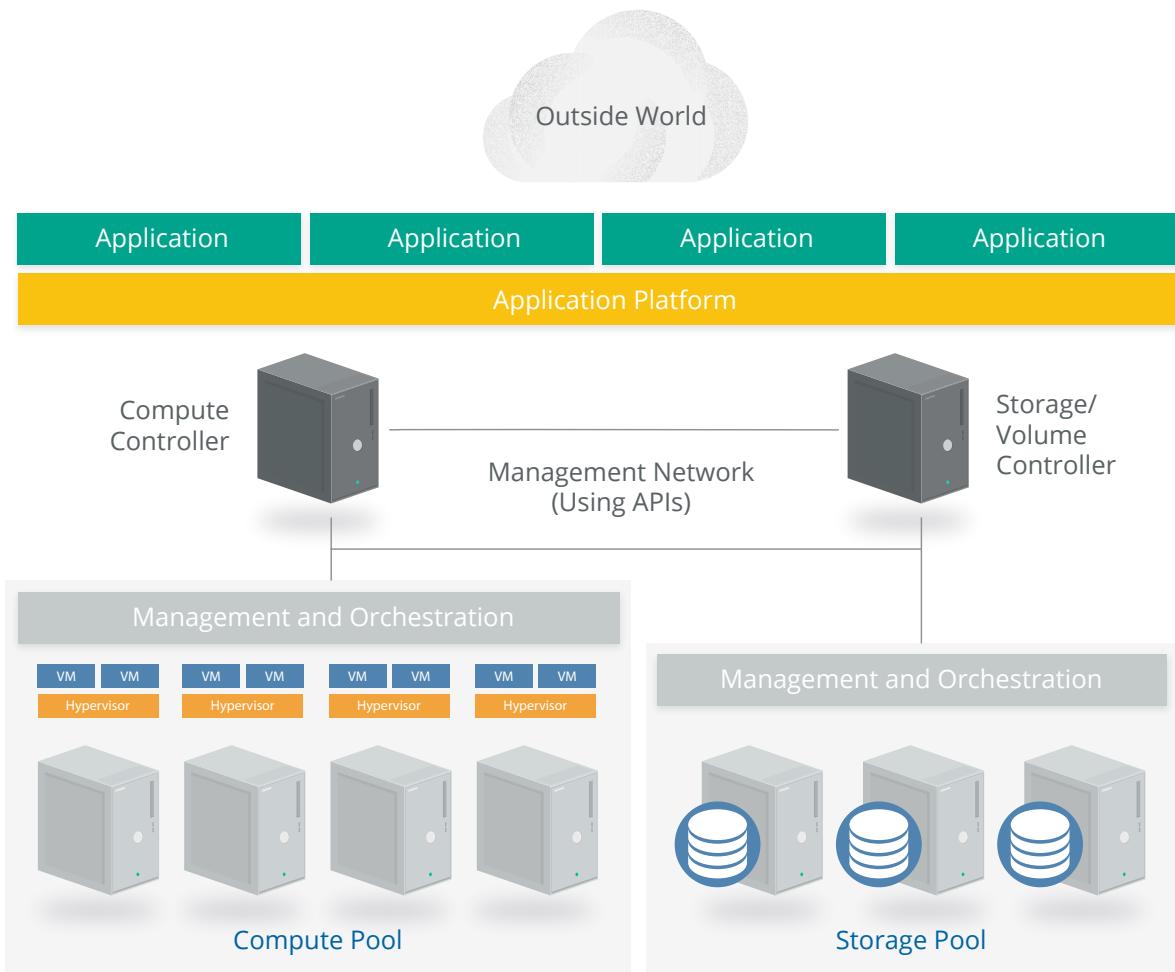
Of all the service models, **PaaS** is the hardest to definitively characterize due to both the wide range of PaaS offerings and the many ways of building PaaS services. PaaS adds an additional layer of integration with application development frameworks, middleware capabilities, and functions such as databases, messaging, and queuing. These services allow developers to build applications on the platform with programming languages and tools that are supported by the stack.

One option, frequently seen in the real world and illustrated in our model, is to build a platform on top of IaaS. A layer of integration and middleware is built on IaaS, then pooled together, orchestrated, and exposed to customers using APIs as PaaS. For example, a Database as a Service could be built by deploying modified database management system software on instances running in IaaS. The customer manages the database via API (and a web console) and accesses it either through the normal database network protocols, or, again, via API.

In PaaS the cloud user only sees the platform, not the underlying infrastructure. In our example, the database expands (or contracts) as needed based on utilization, without the customer having to manage individual servers, networking, patches, etc.

Another example is an application deployment platform. That's a place where developers can load and run application code without managing the underlying resources. Services exist for running nearly any kind of application in any language on PaaS, freeing the developers from configuring and building servers, keeping them up to date, or worrying about complexities like clustering and load balancing.

This simplified architecture diagram shows an application platform (PaaS) running on top of our IaaS architecture:



PaaS doesn't necessarily need to be built on top of IaaS; there is no reason it cannot be a custom-designed stand-alone architecture. The defining characteristic is that consumers access and manage the platform, not the underlying infrastructure (including cloud infrastructure).

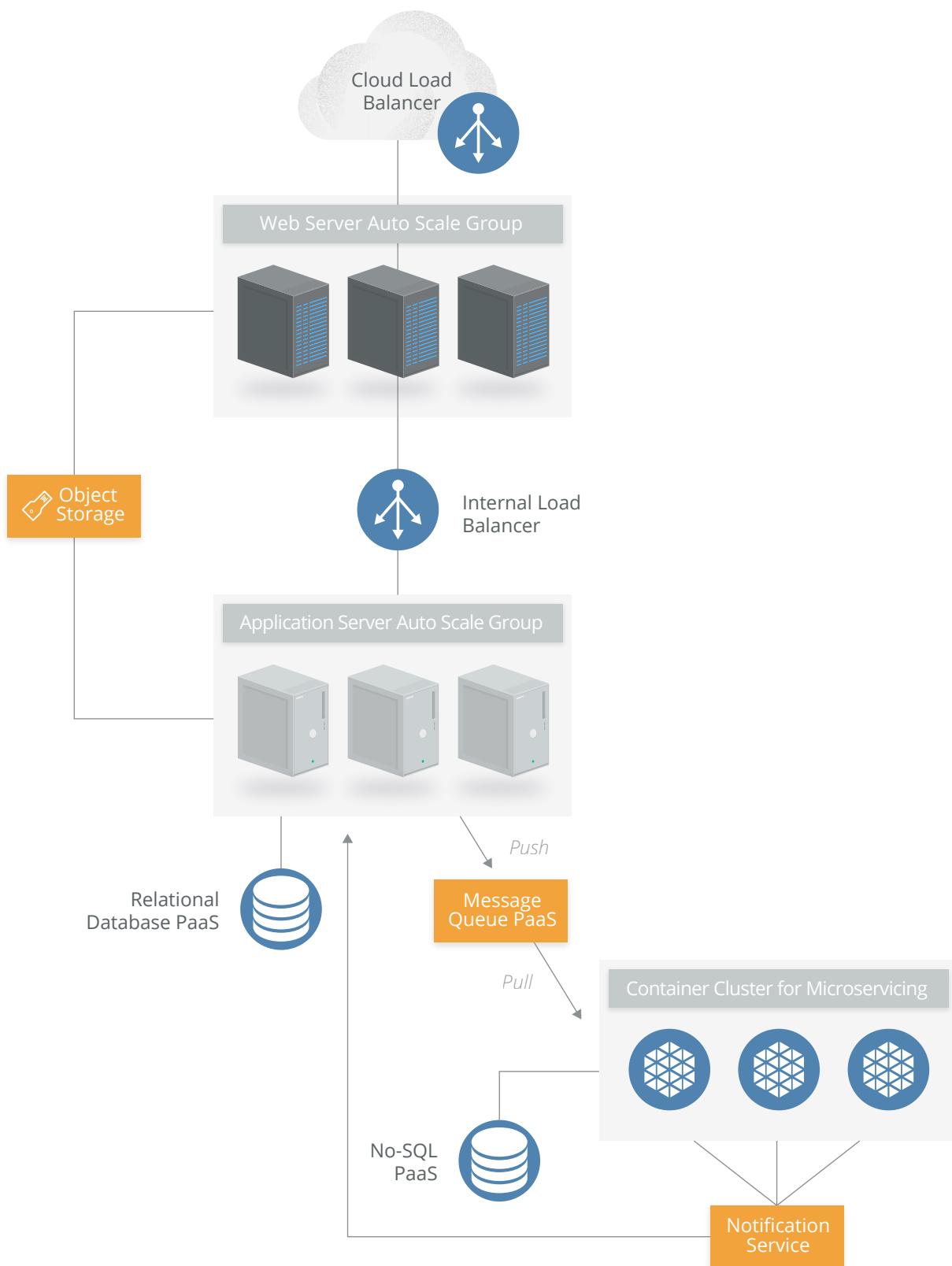
#### 1.1.3.3 Software as a Service

SaaS services are full, multitenant applications, with all the architectural complexities of any large software platform. Many SaaS providers build on top of IaaS and PaaS due to the increased agility, resilience, and (potential) economic benefits.

Most modern cloud applications (SaaS or otherwise) use a combination of IaaS and PaaS, sometimes across different cloud providers. Many also tend to offer public APIs for some (or all) functionality. They often need these to support a variety of clients, especially web browsers and mobile applications.

Thus all SaaS tends to have an application/logic layer and data storage, with an API on top. Then there are one or more presentation layers, often including web browsers, mobile applications, and public API access.

The simplified architecture diagram below is taken from a real SaaS platform, but generalized to remove references to the specific products in use:



## 1.1.4 Logical Model

At a high level, both cloud and traditional computing adhere to a logical model that helps identify different layers based on functionality. This is useful to illustrate the differences between the different computing models themselves:

- *Infrastructure*: The core components of a computing system: compute, network, and storage. The foundation that everything else is built on. The moving parts.
- *Metastructure*: The protocols and mechanisms that provide the interface between the infrastructure layer and the other layers. The glue that ties the technologies and enables management and configuration.
- *Infostructure*: The data and information. Content in a database, file storage, etc.
- *Applistructure*: The applications deployed in the cloud and the underlying application services used to build them. For example, Platform as a Service features like message queues, artificial intelligence analysis, or notification services.

Different security focuses map to the different logical layers. Application security maps to applistructure, data security to infostructure, and infrastructure security to infrastructure.

*The key difference between cloud and traditional computing is the metastructure.* Cloud metastructure includes the management plane components, which are network-enabled and remotely accessible. Another key difference is that, in cloud, you tend to double up on each layer. Infrastructure, for example, includes both the infrastructure used to create the cloud as well as the virtual infrastructure used and managed by the cloud user. In private cloud, the same organization might need to manage both; in public cloud the provider manages the physical infrastructure while the consumer manages their portion of the virtual infrastructure.

As we will discuss later this has profound implications on who is responsible for, and manages, security.

These layers tend to map to different teams, disciplines, and technologies commonly found in IT organizations. While the most obvious and immediate security management differences are in metastructure, cloud differs extensively from traditional computing within each layer. The scale of the differences will depend not only on the cloud platform, but on *how* exactly the cloud user utilizes the platform.

Infostructure

Applistructure

Metastructure

Infrastructure

A vertical sidebar on the left side of the page contains ten icons, each with a thin blue outline, separated by horizontal lines:

- Cloud icon
- Exclamation mark icon
- Search icon
- Document icon
- Server rack icon
- Database icon
- Shield icon
- Laptop icon
- Cloud with gear icon
- Network icon

For example, a cloud-native application that makes heavy utilization of a cloud provider's PaaS products will experience more application differences than the migration of an existing application, with minimal changes, to Infrastructure as a Service.

## 1.2 Cloud Security Scope, Responsibilities, and Models

### 1.2.1 Cloud Security and Compliance Scope and Responsibilities

It might sound simplistic, but cloud security and compliance includes everything a security team is responsible for today, just in the cloud. All the traditional security domains remain, but the *nature of risks, roles and responsibilities, and implementation of controls* change, often dramatically.

Though the overall scope of security and compliance doesn't change, the pieces any given cloud actor is responsible for most certainly do. Think of it this way: Cloud computing is a shared technology model where different organizations are frequently responsible for implementing and managing different parts of the stack. As a result security responsibilities are also distributed across the stack, and thus across the organizations involved.

This is commonly referred to as the *shared responsibility model*. Think of it as a responsibility matrix that depends on the particular cloud provider and feature/product, the service model, and the deployment model.

At a high level, security responsibility maps to the degree of control any given actor has over the architecture stack:

- *Software as a Service*: The cloud provider is responsible for nearly all security, since the cloud user can only access and manage their use of the application, and can't alter how the application works. For example, a SaaS provider is responsible for perimeter security, logging/monitoring/auditing, and application security, while the consumer may only be able to manage authorization and entitlements.
- *Platform as a Service*: The cloud provider is responsible for the security of the platform, while the consumer is responsible for everything they implement on the platform, including how they configure any offered security features. The responsibilities are thus more evenly split. For example, when using a Database as a Service, the provider manages fundamental security, patching, and core configuration, while the cloud user is responsible for everything else, including which security features of the database to use, managing accounts, or even authentication methods.
- *Infrastructure as a Service*: Just like PaaS, the provider is responsible for foundational security, while the cloud user is responsible for everything they build on the infrastructure. Unlike PaaS, this places far more responsibility on the client. For example, the IaaS provider will likely monitor their perimeter for attacks, but the consumer is fully responsible for how they define and implement their virtual network security, based on the tools available on the service.



These roles are further complicated when using cloud brokers or other intermediaries and partners.

*The most important security consideration is knowing exactly who is responsible for what in any given cloud project.* It's less important if any particular cloud provider offers a specific security control, as long as you know precisely what they do offer and how it works. You can fill the gaps with your own controls, or choose a different provider if you can't close the controls gap. Your ability to do this is very high for IaaS, and less so for SaaS.

This is the essence of the security relationship between a cloud provider and consumer. What does the provider do? What does the consumer need to do? Does the cloud provider enable the consumer to do what they need to? What is guaranteed in the contract and service level agreements, and what is implied by the documentation and specifics of the technology?

This shared responsibility model directly correlates to two recommendations:

- *Cloud providers* should clearly document their internal security controls and customer security features so the cloud user can make an informed decision. Providers should also properly design and implement those controls.
- *Cloud users* should, for any given cloud project, build a responsibilities matrix to document who is implementing which controls and how. This should also align with any necessary compliance standards.

The Cloud Security Alliance provides two tools to help meet these requirements:

- The **Consensus Assessments Initiative Questionnaire (CAIQ)**. A standard template for cloud providers to document their security and compliance controls.
- The **Cloud Controls Matrix (CCM)**, which lists cloud security controls and maps them to multiple security and compliance standards. The CCM can also be used to document security responsibilities.

Both documents will need tuning for specific organizational and project requirements, but provide a comprehensive starting template and can be especially useful for ensuring compliance requirements are met.

## 1.2.2 Cloud Security Models

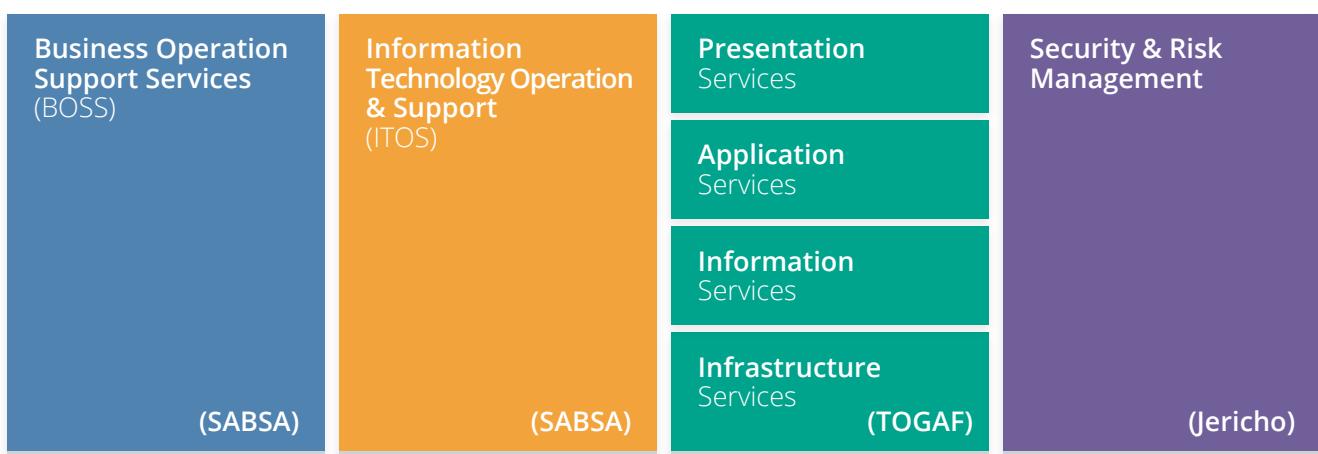
Cloud security models are tools to help guide security decisions. The term “model” can be used a little nebulously, so for our purposes we break out the following types:

- *Conceptual models or frameworks* include visualizations and descriptions used to explain cloud security concepts and principles, such as the CSA logical model in this document.
- *Controls models or frameworks* categorize and detail specific cloud security controls or categories of controls, such as the CSA CCM.
- *Reference architectures* are templates for implementing cloud security, typically generalized (e.g. an IaaS security reference architecture). They can be very abstract, bordering on conceptual, or quite detailed, down to specific controls and functions.
- *Design patterns* are reusable solutions to particular problems. In security, an example is IaaS log management. As with reference architectures, they can be more or less abstract or specific, even down to common implementation patterns on particular cloud platforms.

The lines between these models often blur and overlap, depending on the goals of the developer of the model. Even lumping these all together under the heading “model” is probably inaccurate, but since we see the terms used so interchangeably across different sources, it makes sense to group them.

The CSA has reviewed and recommends the following models:

- The [CSA Enterprise Architecture](#)
- The [CSA Cloud Controls Matrix](#)
- The NIST draft [Cloud Computing Security Reference Architecture \(NIST Special Publication 500-299\)](#), which includes conceptual models, reference architectures, and a controls framework.
- [ISO/IEC FDIS 27017 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services](#).



Throughout this Guidance we also refer to other domain-specific models.

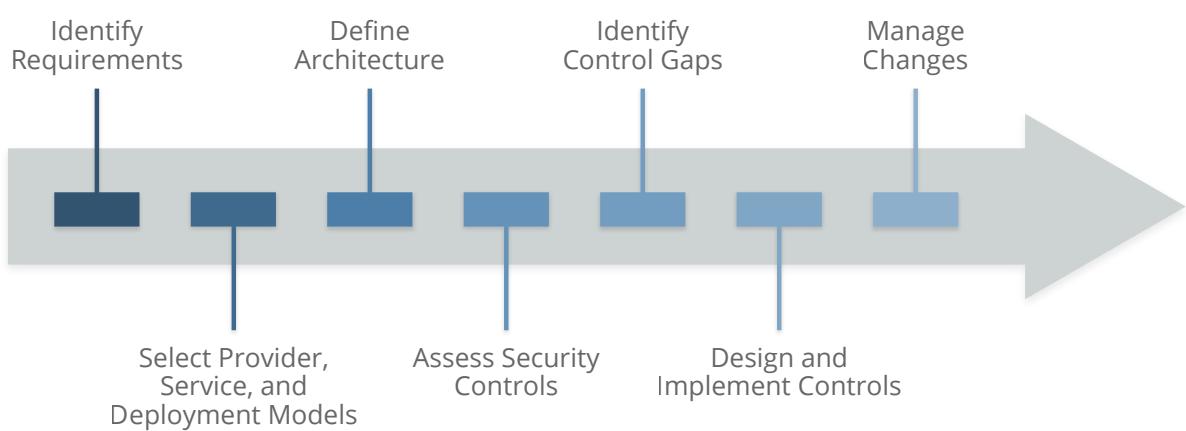
### 1.2.2.1 A Simple Cloud Security Process Model

While the implementation details, necessary controls, specific processes, and various reference architectures and design models vary greatly depending on the specific cloud project, there is a relatively straightforward, high-level process for managing cloud security:

- Identify necessary security and compliance requirements, and any existing controls.
- Select your cloud provider, service, and deployment models.
- Define the architecture.
- Assess the security controls.
- Identify control gaps.
- Design and implement controls to fill the gaps.
- Manage changes over time.

Since different cloud projects, even on a single provider, will likely leverage entirely different sets of configurations and technologies, each project should be evaluated on its own merits. For example, the security controls for an application deployed on pure IaaS in one provider may look very different than a similar project that instead uses more PaaS from that same provider.

The key is to identify requirements, design the architecture, and then identify the gaps based on the capabilities of the underlying cloud platform. That's why you need to know the cloud provider and architecture *before* you start translating security requirements into controls.



## 1.3 Areas of Critical Focus

The 13 other domains which comprise the remainder of the CSA Guidance highlight areas of concern for cloud computing and are tuned to address both the strategic and tactical security “pain points” within a cloud environment, and can be applied to any combination of cloud service and deployment model.

The domains are divided into two broad categories: governance and operations. The governance domains are broad and address strategic and policy issues within a cloud computing environment, while the operational domains focus on more tactical security concerns and implementation within the architecture.

### 1.3.1 Governing in the Cloud

Domain	Title	Description
2	 Governance and Enterprise Risk Management	The ability of an organization to govern and measure enterprise risk introduced by cloud computing. Items such as legal precedence for agreement breaches, ability of user organizations to adequately assess risk of a cloud provider, responsibility to protect sensitive data when both user and provider may be at fault, and how international boundaries may affect these issues.
3	 Legal Issues: Contracts and Electronic Discovery	Potential legal issues when using cloud computing. Issues touched on in this section include protection requirements for information and computer systems, security breach disclosure laws, regulatory requirements, privacy requirements, international laws, etc.
4	 Compliance and Audit Management	Maintaining and proving compliance when using cloud computing. Issues dealing with evaluating how cloud computing affects compliance with internal security policies, as well as various compliance requirements (regulatory, legislative, and otherwise) are discussed here. This domain includes some direction on proving compliance during an audit.
5	 Information Governance	Governing data that is placed in the cloud. Items surrounding the identification and control of data in the cloud, as well as compensating controls that can be used to deal with the loss of physical control when moving data to the cloud, are discussed here. Other items, such as who is responsible for data confidentiality, integrity, and availability are mentioned.

### 1.3.2 Operating in the Cloud

Domain	Title	Description
6	Management Plane and Business Continuity	Securing the management plane and administrative interfaces used when accessing the cloud, including both web consoles and APIs. Ensuring business continuity for cloud deployments.
7	Infrastructure Security	Core cloud infrastructure security, including networking, workload security, and hybrid cloud considerations. This domain also includes security fundamentals for private clouds.
8	Virtualization and Containers	Security for hypervisors, containers, and Software Defined Networks.
9	Incident Response, Notification and Remediation	Proper and adequate incident detection, response, notification, and remediation. This attempts to address items that should be in place at both provider and user levels to enable proper incident handling and forensics. This domain will help you understand the complexities the cloud brings to your current incident-handling program.
10	Application Security	Securing application software that is running on or being developed in the cloud. This includes items such as whether it's appropriate to migrate or design an application to run in the cloud, and if so, what type of cloud platform is most appropriate (SaaS, PaaS, or IaaS).
11	Data Security and Encryption	Implementing data security and encryption, and ensuring scalable key management.
12	Identity, Entitlement, and Access Management	Managing identities and leveraging directory services to provide access control. The focus is on issues encountered when extending an organization's identity into the cloud. This section provides insight into assessing an organization's readiness to conduct cloud-based Identity, Entitlement, and Access Management (IdEA).
13	Security as a Service	Providing third-party-facilitated security assurance, incident management, compliance attestation, and identity and access oversight.
14	Related Technologies	Established and emerging technologies with a close relationship to cloud computing, including Big Data, Internet of Things, and mobile computing.

## 1.4 Recommendations

---

- Understand the differences between cloud computing and traditional infrastructure or virtualization, and how *abstraction* and *automation* impact security.
- Become familiar with the NIST model for cloud computing and the CSA reference architecture.
- Use tools such as the CSA Consensus Assessments Initiative Questionnaire (CAIQ) to evaluate and compare cloud providers.
- Cloud providers should clearly document their security controls and features and publish them using tools like the CSA CAIQ.
- Use tools like the CSA Cloud Controls Matrix to assess and document cloud project security and compliance requirements and controls, as well as who is responsible for each.
- Use a cloud security process model to select providers, design architectures, identify control gaps, and implement security and compliance controls.

## 1.5 Credits

---

- Reference architecture and logical model based on the work of Christofer Hoff

# DOMAIN 2

# Governance and Enterprise Risk Management



## 2.0 Introduction

Governance and risk management are incredibly broad topics. This guidance focuses on how they change in cloud computing; it is not and should not be considered a primer or comprehensive exploration of those topics outside of cloud.

For security professionals, cloud computing impacts four areas of governance and risk management:

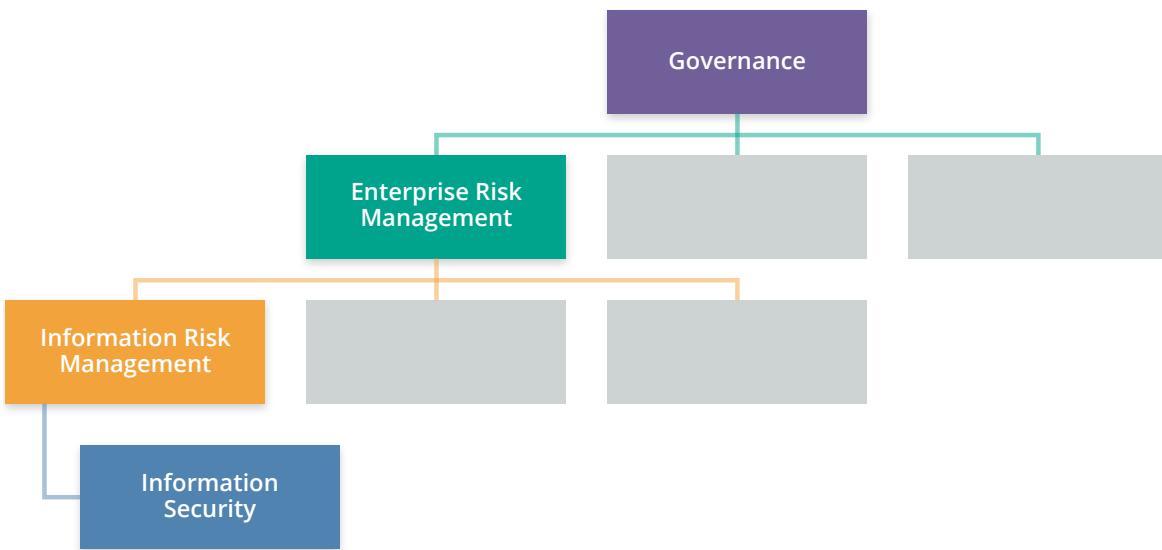
- *Governance* includes the policy, process, and internal controls that comprise how an organization is run. Everything from the structures and policies to the leadership and other mechanisms for management.

For more information on governance please see

- \* [ISO/IEC 38500:2015 - Information Technology - Governance of IT for the organization](#)
- \* [ISACA - COBIT - A Business Framework for the Governance and Management of Enterprise IT](#)
- \* [ISO/IEC 27014:2013 - Information Technology - Security techniques - Governance of information security](#)

- *Enterprise risk management* includes managing overall risk for the organization, aligned to the organization's governance and risk tolerance. Enterprise risk management includes all areas of risk, not merely those concerned with technology.
- *Information risk management* covers managing the risk to information, including information technology. Organizations face all sorts of risks, from financial to physical, and information is only one of multiple assets an organization needs to manage.
- *Information security* is the tools and practices to manage risk to information. Information security isn't the be-all and end-all of managing information risks; policies, contracts, insurance, and other mechanisms also play a role (including physical security for non-digital information). However, a—if not *the*—primary role of information security is to provide the processes and controls to protect electronic information and the systems we use to access it.

In a simplified hierarchy, information security is a tool of information risk management, which is a tool of enterprise risk management, which is a tool of governance. The four are all closely related but require individual focus, processes, and tools.



2.1: A Simplified Risk and Governance Hierarchy

Legal issues and compliance are covered in Domains 3 and 4, respectively. Information risk management and data governance are covered in Domain 5. Information security is essentially the rest of this guidance.

## 2.1 Overview

### 2.1.1 Governance

Cloud computing affects governance, since it either introduces a third party into the process (in the case of public cloud or hosted private cloud) or potentially alters internal governance structures in the case of self-hosted private cloud. The primary issue to remember when governing cloud computing is that *an organization can never outsource responsibility for governance*, even when using external providers. This is always true, cloud or not, but is useful to keep in mind when navigating cloud computing's concepts of shared responsibility models.

Cloud service providers try to leverage economies of scale to manage costs and enable capabilities. This means creating extremely standardized services (including contracts and service level agreements) that are consistent across all customers. Governance models can't necessarily treat cloud providers the same way they'd treat dedicated external service providers, which typically customize their offerings, including legal agreements, for each client.

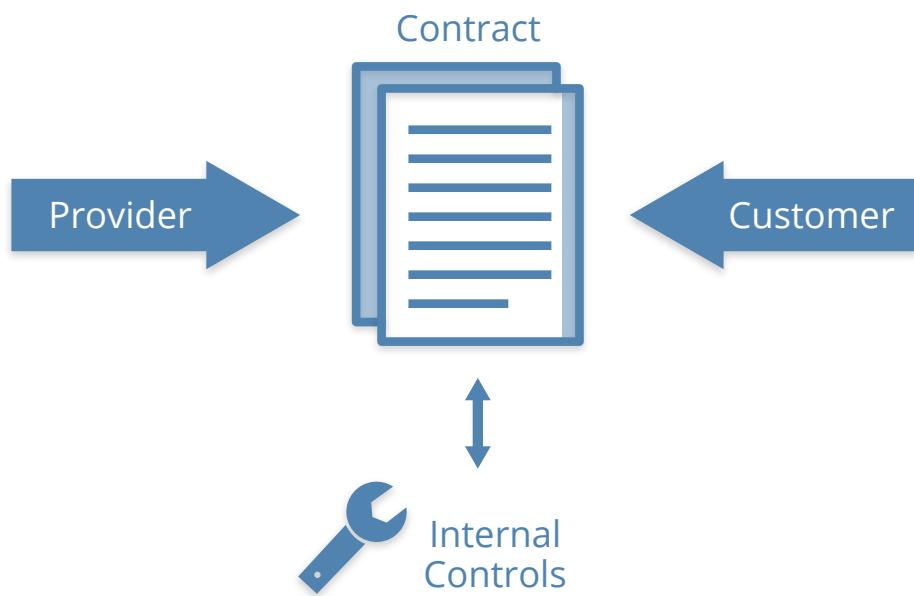
Cloud computing changes the *responsibilities* and mechanisms for implementing and managing governance. Responsibilities and mechanisms for governance are defined in the contract, as with

any business relationship. If the area of concern isn't in the contract, there are no mechanisms available to enforce, and there is a governance gap. Governance gaps don't necessarily exclude using the provider, but they do require the customer to adjust their own processes to close the gaps or accept the associated risks.

#### 2.1.1.1 Tools of Cloud Governance

As with any other area, there are specific management tools used for governance. This list focuses more on tools for external providers, but these same tools can often be used internally for private deployments:

- *Contracts*: The primary tool of governance is the contract between a cloud provider and a cloud customer (this is true for public and private cloud). The contract is your only guarantee of any level of service or commitment—assuming there is no breach of contract, which tosses everything into a legal scenario. Contracts are the primary tool to extend governance into business partners and providers.



Contracts define the relationship between providers and customers and are the primary tool for customers to extend governance to their suppliers.

- *Supplier (cloud provider) Assessments*: These assessments are performed by the potential cloud customer using available information and allowed processes/techniques. They combine contractual and manual research with third-party attestations (legal statements often used to communicate the results of an assessment or audit) and technical research. They are very similar to any supplier assessment and can include aspects like financial viability, history, feature offerings, third-party attestations, feedback from peers, and so on. More detail on assessments is covered later in this Domain and in Domain 4.

- *Compliance reporting:* Compliance reporting includes all the documentation on a provider's internal (i.e. self) and external compliance assessments. They are the reports from *audits of controls*, which an organization can perform themselves, a customer can perform on a provider (although this usually isn't an option in cloud), or have performed by a trusted third party. Third-party audits and assessments are preferred since they provide independent validation (assuming you trust the third party).

Compliance reports are often available to cloud prospects and customers but may only be available under NDA or to contracted customers. This is often required by the firm that performed the audit and isn't necessarily something that's completely under the control of the cloud provider.

Assessments and audits should be based on existing standards (of which there are many). It's critical to understand the scope, not just the standard used. Standards like the SSAE 16 have a defined scope, which includes both *what* is assessed (e.g. which of the provider's services) as well as *which controls* are assessed. A provider can thus "pass" an audit that doesn't include any security controls, which isn't overly useful for security and risk managers. Also consider the transitive trust required to treat a third-party assessment as equivalent to the activities that you might undertake when doing your own assessment. Not all audit firms (or auditors) are created equal and the experience, history, and qualifications of the firm should be included in your governance decisions.

The [Cloud Security Alliance STAR Registry](#) is an assurance program and documentation registry for cloud provider assessments based on the CSA Cloud Controls Matrix and Consensus Assessments Initiative Questionnaire. Some providers also disclose documentation for additional certifications and assessments (including self-assessments).

### **2.1.2 Enterprise Risk Management**

Enterprise Risk Management (ERM) is the overall management of risk for an organization. As with governance, the contract defines the roles and responsibilities for risk management between a cloud provider and a cloud customer. And, as with governance, you can never outsource your overall responsibility and accountability for risk management to an external provider.

For more on risk management see

- \* [ISO 31000:2009 - Risk management – Principles and guidelines](#)
- \* [ISO/IEC 31010:2009 - Risk management – Risk assessment techniques](#)
- \* [NIST Special Publication 800-37 Revision 1](updated June 5, 2014) (<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf>)

Risk management in cloud is based on the *shared responsibilities model* (which we most often discuss in reference to security). The cloud provider accepts some responsibility for certain risks, and the cloud customer is responsible for anything beyond that. This is especially evident as you evaluate differences between the service models, where the provider manages more risks in SaaS and the consumer more in IaaS. But, again, the cloud user is ultimately responsible for ownership of the risks; they only pass on some of the *risk management* to the cloud provider. This holds true even



with a self-hosted private cloud; in those situations an organizational unit is passing on some of their risk management to the internal cloud provider instead of an external party, and internal SLAs and procedures replace external contracts.

ERM relies on good contracts and documentation to know where the division of responsibilities and potential for untreated risk lie. Whereas governance is nearly exclusively focused on contracts, risk management can delve deeper into the technology and process capabilities of the provider, based on their documentation. For example, a contract will rarely define how network security is actually implemented. Review of the provider's documentation will provide much more information to help with an effective risk decision.

*Risk tolerance* is the amount of risk that the leadership and stakeholders of an organization are willing to accept. It varies based on asset and you shouldn't make a blanket risk decision about a particular provider; rather, assessments should align with the value and requirements of the assets involved. Just because a public cloud provider is external and a consumer might be concerned with shared infrastructure for some assets doesn't mean it isn't within risk tolerance for all assets. Over time this means that, practically speaking, you will build out a matrix of cloud services along with which types of assets are allowed in those services. Moving to the cloud doesn't change your risk tolerance, it just changes how risk is managed.

### **2.1.3The Effects of Service Model and Deployment Model**

In considering the various options available not only in Cloud Service Providers but also in the fundamental delivery of cloud services, attention must be paid to how the Service and Deployment models affect the ability to manage governance and risk.

#### **2.1.3.1 Service Models**

##### **Software as a Service (SaaS)**

In the majority of cases, SaaS presents the most critical example of the need for a negotiated contract. Such a contract will protect the ability to govern or validate risk as it relates to data stored, processed, and transmitted with and in the application. SaaS providers tend to cluster at either end of the size/capability spectrum and the likelihood of a negotiated contract is much higher when dealing with a small SaaS provider. Unfortunately, many small SaaS providers are not able to operate at a level of sophistication that meets or exceeds customer governance and risk management capabilities. In concrete terms, the entire level of visibility into the actual operation of the infrastructure providing the SaaS application is limited to solely what is exposed in the user interface developed by the Cloud Provider.

##### **Platform as a Service (PaaS)**

Continuing through the Service Models, the level of detail that is available (and the consequential ability to self-manage governance and risk issues) increases. The likelihood of a fully negotiated contract is likely lower here than with either of the other service models. That's because the core driver for most PaaS is to deliver a single capability with very high efficiency.

PaaS is typically delivered with a rich API, and many PaaS providers have enabled the collection of

some of the data necessary to prove that SLAs are being adhered to. That said, the customer is still in the position of having to exercise a significant effort in determining whether contract stipulations are effectively providing the level of control or support required to enable governance or risk management.

### Infrastructure as a Service (IaaS)

Infrastructure as a Service represents the closest that Cloud comes to a traditional data center (or even a traditional outsourced managed data center), and the good news is that the vast majority of existing

governance and risk management activities that organizations have already built and utilize are directly transferable. There are, however, new complexities related to the underlying orchestration and management layers, as described in Domain 1, that enable the infrastructure which are often overlooked.

In many ways, the governance and risk management of that orchestration and management layer is consistent with the underlying infrastructure (network, power, HVAC, etc.) of a traditional data center. The same governance and risk management issues are present, but the exposure of those systems is sufficiently different that changes to the existing process are required. For example, controlling who can make network configuration changes shifts from accounts on individual devices to the cloud management plane.

#### 2.1.3.2 Deployment Models



Cloud customers have a reduced ability to govern operations in a public cloud since the provider is responsible for the management and governance of their infrastructure, employees, and everything else. The customers also often have reduced ability to negotiate contracts, which impacts how they extend their governance model into the cloud. Inflexible contracts are a natural property of multitenancy: Providers can't necessarily adjust contracts and operations for each customer as everything runs on one set of resources, using one set of processes. Adapting for different customers increases costs, causing a trade-off, and often that's the dividing line between using public and private cloud. Hosted private cloud allows full customization, but at increased costs due to the loss of the economies of scale.

This doesn't mean you shouldn't try to negotiate your contract, but recognize that this isn't always possible; instead, you'll need to either choose a different provider (which may actually be less secure), or adjust your needs and use alternate governance mechanisms to mitigate concerns.

To use an analogy, think of a shipping service. When you use a common carrier/provider you don't get to define their operations. You put your sensitive documents in a package and entrust them to meet their obligations to deliver it safely, securely, and within the expected Service Level Agreement.



Public cloud isn't the only model that impacts governance; even private cloud will have an effect. If an organization allows a third party to own and/or manage the private cloud (which is very common), this is similar to how governance affects any outsourced provider. There will be shared responsibilities with obligations that are defined in the contract.

Although you will likely have more control over contractual terms, it's still important to ensure they cover the needed governance mechanisms. As opposed to a public provider—which has various incentives to keep its service well-documented and at particular standard levels of performance, functionality, and competitiveness—a hosted private cloud may only offer exactly what is in the contract, with everything else at extra cost. This *must* be considered and accounted for in negotiations, with clauses to guarantee that the platform itself remains up to date and competitive. For example, by requiring the vendor to update to the latest version of the private cloud platform within a certain time period of release and after *your* sign-off.

With a self-hosted private cloud governance will focus on internal service level agreements for the cloud users (business or other organizational units) and chargeback and billing models for providing access to the cloud.



When contemplating **hybrid cloud environments**, the governance strategy must consider the minimum common set of controls comprised of the Cloud Service Provider's contract and the organization's internal governance agreements. The cloud user is connecting either two cloud environments or a cloud environment and a data center. In either case the overall governance is the intersection of those two models. For example, if you connect your data center to your cloud over a dedicated network link you need to account for governance issues that will span both environments.

Since **community clouds** are a shared platform with multiple organizations, but are not public, governance extends to the relationships with those members of the community, not just the provider and the customer. It's a mix of how you would approach public cloud and hosted private cloud governance, where the overall tools of governance and contracts will have some of the economies of scale of a public cloud provider, but be tunable based on community consensus, as with a hosted private cloud. This also includes community membership relations, financial relationships, and how to respond when a member leaves the community.

#### 2.1.3.3 Cloud Risk Management Trade-Offs

There are advantages and disadvantages to managing enterprise risk for cloud deployments. These factors are, as you would expect, more pronounced for public cloud and hosted private cloud:

- There is less physical control over assets and their controls and processes. You don't physically control the infrastructure or the provider's internal processes.
- There is a greater reliance on contracts, audits, and assessments, as you lack day-to-day visibility or management.
- This creates an increased requirement for proactive management of relationship and adherence to contracts, which extends beyond the initial contract signing and audits. Cloud providers also constantly evolve their products and services to remain competitive and these ongoing innovations might exceed, strain, or not be covered by existing agreements and assessments.
- Cloud customers have a reduced need (and associated reduction in costs) to manage risks that the cloud provider accepts under the shared responsibility model. You haven't

 outsourced accountability for managing the risk, but you can certainly outsource the management of some risks.

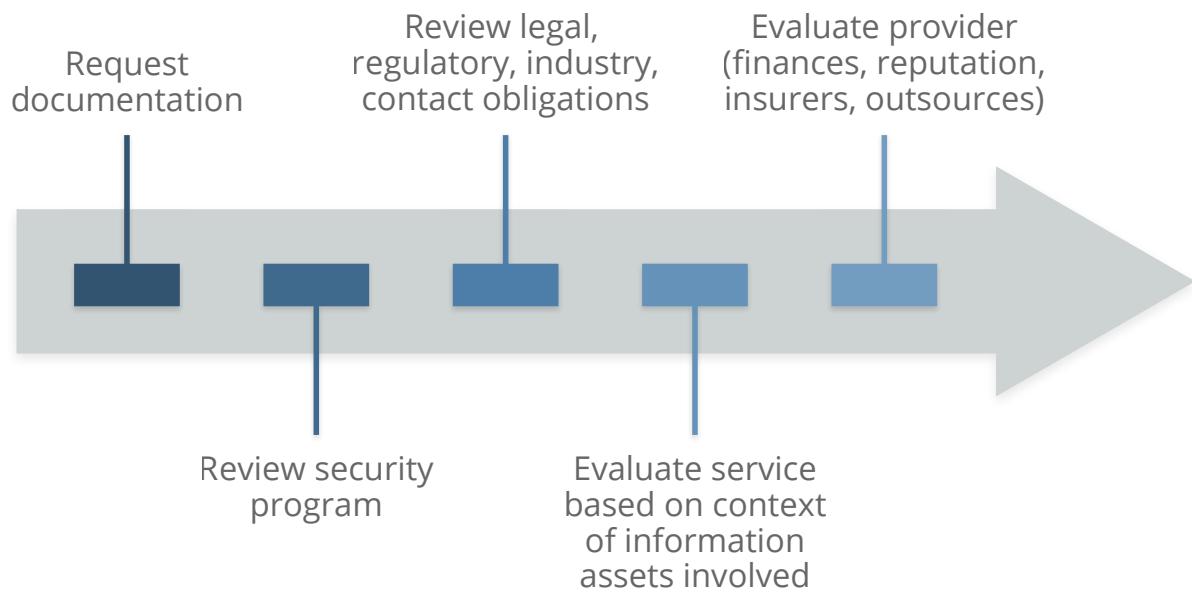


#### 2.1.3.4 Cloud Risk Management Tools

  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
The following processes help form the foundation of managing risk in cloud computing deployments. One of the core tenants of risk management is that you can *manage, transfer, accept, or avoid* risks. But everything starts with a proper assessment.

The supplier assessment sets the groundwork for the cloud risk management program:

- Request or acquire documentation.
- Review their security program and documentation.
- Review any legal, regulatory, contractual, and jurisdictional requirements for both the provider and yourself. (See the Domain 3: Legal for more.)
- Evaluate the contracted service in the context of your information assets.
- Separately evaluate the overall provider, such as finances/stability, reputation, and outsourcers.



#### Supplier Assessment Process

Periodically review audits and assessments to ensure they are up to date:

- Don't assume all services from a particular provider meet the same audit/assessment standards. They can vary.
- Periodic assessments should be scheduled and *automated* if possible.

After reviewing and understanding what risks the cloud provider manages, what remains is residual risk. Residual risk may often be managed by controls that you implement (e.g. encryption). The availability and specific implementation of risk controls vary greatly across cloud providers, particular

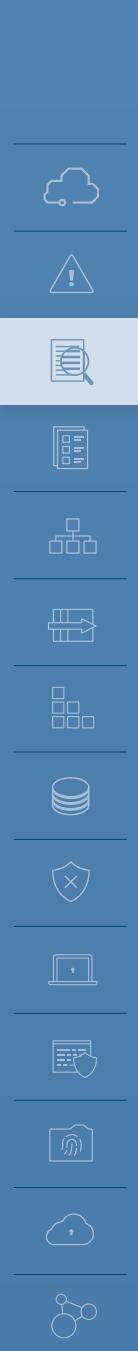


services/features, service models, and deployment models. If, after all your assessments and the controls that you implement yourself there is still residual risk your only options are to transfer it, accept the risk, or avoid it.

Risk transfer, most often enabled by insurance, is an imperfect mechanism, especially for information risks. It can compensate some of the financial loss associated with a primary loss event, but won't help with a secondary loss event (like loss of customers)—especially an intangible or difficult to quantify loss, such as reputation damage. From the perspective of insurance carriers, cyber-insurance is also a nascent field without the depth of actuarial tables used for other forms of insurance, like those for fire or flooding, and even the financial compensation may not match the costs associated with the primary loss event. Understand the limits.

## 2.2 Recommendations

- Identify the shared responsibilities of security and risk management based on the chosen cloud deployment and service model. Develop a Cloud Governance Framework/Model as per relevant industry best practices, global standards, and regulations like CSA CCM, COBIT 5, NIST RMF, ISO/IEC 27017, HIPAA, PCI DSS, EU GDPR, etc.
- Understand how a contract affects your governance framework/model.
  - Obtain and review contracts (and any referenced documents) before entering into an agreement.
  - Don't assume that you can effectively negotiate contracts with a cloud provider—but this also shouldn't necessarily stop you from using that provider.
  - If a contract can't be effectively negotiated and you perceive an unacceptable risk, consider alternate mechanisms to manage that risk (e.g. monitoring or encryption).
- Develop a process for cloud provider assessments.
  - This should include:
    - Contract review.
    - Self-reported compliance review.
    - Documentation and policies.
    - Available audits and assessments.
    - Service reviews adapting to the customer's requirements.
    - Strong change-management policies to monitor changes in the organization's use of the cloud services.
  - Cloud provider re-assessments should occur on a scheduled basis and be automated if possible.
- Cloud providers should offer easy access to documentation and reports needed by cloud prospects for assessments.
  - For example, the CSA STAR registry.
- Align risk requirements to the specific assets involved and the risk tolerance for those assets.
- Create a specific risk management and risk acceptance/mitigation methodology to assess the risks of every solution in the space
- Use controls to manage residual risks.
  - If residual risks remain, choose to accept or avoid the risks.
- Use tooling to track approved providers based on asset type (e.g. linked to data classification), cloud usage, and management.



# DOMAIN 3

# Legal Issues, Contracts and Electronic Discovery



## 3.0 Introduction

This domain highlights some of the legal issues raised by moving data to the cloud; contracting with cloud service providers; and handling electronic discovery requests in litigation. Our overview here cannot address every potential legal situation. To address your specific issues, you should consult with legal counsel in the jurisdiction(s) in which you intend to operate and/or in which your customers reside. In addition, be aware that laws and regulations change frequently, and thus you should verify the relevancy of information contained in this domain before relying on it. Domain 3 is concerned primarily with the legal implications of public cloud computing and third party-hosted private clouds. Although this domain includes some aspects of data governance and audit/compliance, those topics are covered in more depth in domains 4 and 5.

Specific areas covered in this domain include the following:

- Legal issues
- Cloud service agreements (contracts)
- Third-party access to electronic documents stored in the cloud

## 3.1 Overview

### 3.1.1 Legal Frameworks Governing Data Protection and Privacy

Throughout the world, many countries have adopted legal frameworks requiring public and private organizations to safeguard the privacy of personal data and the security of information and computer systems. Most of these laws are based in part on the fair information privacy principles developed in the late 1960s and 1970s and later clarified and expanded in the Privacy and Security Guidelines of the Organization for Economic Cooperation and Development (OECD).

Under these laws, the data controller (typically the entity that has the primary relationship with an individual) is prohibited from collecting and processing personal data unless certain criteria are met. For example, if the data subject has consented to the collection and proposed uses of his or

her data, then the controller may collect and process data, according to the consent agreement. These laws define numerous obligations, such as confidentiality and security obligations, for the entities that access personal data. When entrusting a third party to process data on its behalf (a data processor), a data controller remains responsible for the collection and processing of that data. The data controller is required to ensure that any such third parties take adequate technical and organizational security measures to safeguard the data.

Despite a common theme, countries on all continents have developed data protection regimes that occasionally conflict with each other. As a result, cloud providers and cloud users operating in multiple regions struggle to meet compliance requirements.

In many cases, the laws of different countries might apply concurrently, in accordance with the following:

- The location of the cloud provider
- The location of the cloud user
- The location of the data subject
- The location of the servers
- The legal jurisdiction of the contract between parties, which may be different than the locations of any of the parties involved
- Any treaties or other legal frameworks between those various locations



*Applicable legal requirements will vary tremendously based on the various jurisdictions and legal entities and frameworks involved.*



### 3.1.1.1 Common Themes

Many countries have adopted national or omnibus laws (applying to all categories of personal data) or sectoral laws (applying to specified categories of data) that are intended to protect the privacy of individuals.

### 3.1.1.2 Required Security Measures

These laws frequently contain provisions requiring the adoption of security measures, acknowledging that ensuring the security of personal data is essential to ensuring the protection of individual privacy. Concurrently, companies may also be expected to adopt reasonable technical, physical, and administrative measures in order to protect a wide range of data, including personal data, financial data, trade secrets, and other sensitive company data from loss, misuse or alteration.

### 3.1.1.3 Restrictions to Cross-border Data Transfers

Many countries prohibit or restrict the transfer of information out of their borders. In most cases, the transfer is permitted only if the country to which the data is transferred offers an “adequate level of protection” (as defined in the relevant national law) of personal information and privacy rights of affected individuals. The purpose of this adequacy requirement is to ensure the individuals whose data is transferred across borders will remain as protected as they were via policies afforded to them before the transfer of data.

Alternatively, the data importer and exporter may need to sign a contract insuring the maintenance of privacy rights for data subjects. Depending on the country, the requirements for ensuring this adequate protection may be complex and stringent. In some cases, it may be necessary to obtain prior permission of the local Data Protection Commissioner before transferring data in or out of the country.

In addition, some countries are beginning to require that certain data be stored within their territory. This is the case, for example, with the new data localization laws of Russia and China, which require that specified personal data pertaining to individuals residing in their countries be stored within the country's borders.



### 3.1.1.4 Regional Examples

Below are examples of information privacy and security laws and legal frameworks in effect in numerous parts of the world.



#### Australia

In Australia, two key laws provide protection to consumers of cloud services: the Privacy Act of? 1988 (Privacy Act) and the Australian Consumer Law (ACL) of what year?. The Privacy Act includes 13 Australian Privacy Principles (APPs), which apply to all private sector and not-for-profit organizations with an annual turnover of more than AUD 3 million, all private health service providers, and some small businesses.

In February 2017, Australia amended its 1988 Privacy Act to require companies to notify affected Australian residents and the Australian Information Commissioner in the event of a breach of security. A breach of security must be reported if (a) there is unauthorized access or disclosure of personal information that would be likely to result in serious harm; or (b) personal information is lost in circumstances where unauthorized access or disclosure is likely to occur, and if it did occur, it would be likely to result in serious harm to any of the individuals to whom the information relates.

The ACL protects consumers from false or misleading contracts and poor conduct from providers, such as failed breach notifications. The Privacy Act can apply to Australian customers, even if the cloud service provider is based elsewhere, and even if other laws are stated in a contract.

#### China

Over the past few years, China has accelerated the pace of its adoption of legal structures to address the privacy and security of personal and company information. Its 2017 Cyber Security Law governs the operations of network operators and critical information infrastructure operators. In May 2017, proposed Measures on the Security of Cross-Border Transfers of Personal Information and Important Data were published by the Chinese government and are currently being evaluated for potential implementation.

The 2017 Cyber Security Law requires network operators to comply with a series of security requirements, including the design and adoption of information security measures; the formulation of cyber security emergency response plans; and assistance and support necessary to investigative authorities, where necessary, for protecting national security and investigating crimes. The law



requires providers of network products and services to inform users about known security defects and bugs and to report such defects and bugs to relevant authorities.

The Cyber Security Law imposes a series of security obligations to operators of critical information infrastructure, including internal organization, training, data backup; emergency response requirements, security inspections and annual assessments of cyber security risks; and reporting to relevant authorities. In addition, the law includes a data localization provision, which requires that personal information and other important data be stored within the territories of the People's Republic of China.

During the second quarter of 2017, China issued Draft Regulations on Cross Border Data Transfers to supplement the Cyber Security Law. These regulations would go beyond the working of the Cyber Security Law, and expand its scope. The draft regulations would impose new security review requirements on companies that contemplate sending data overseas. They would expand data localization requirements, and increase the categories of information that must be stored only on China's borders. In particular, they would include personal information and important data collected by any network operators. The cybersecurity and privacy landscape as defined under the Cyber Security Law is in evolution, and has not yet stabilized.

## Japan

In Japan, the Act on the Protection of Personal Information (APPI) requires the private sector to protect personal information and data securely. There are several other national laws, such as the Law on the Protection of Personal Information Held by Administrative Organs and laws pertaining to specific sectors, such as the healthcare industry. Profession-specific laws, such as the Medical Practitioners' Act; the Act on Public Health Nurses, Midwives and Nurses; and the Pharmacist Act, require registered health professionals to maintain the confidentiality of patient information.

Beginning in September 2017, amendments to the APPI law will limit the ability to transfer personal data to third parties, with prior consent of the data subject generally being required to transfer data to a third party. Consent to the transfer is not required if the country of destination has an established framework for the protection of personal information that meets the standard specified by the Personal Information Protection Commission.

## Russia

The Russian data protection laws contain significant restrictions on data processing, including a requirement for consent for most forms of data processing. However, the most important aspect of the Russian legal framework regarding the handling of personal information is its data localization law. Since September 2015, companies are required to store personal data of Russian citizens within Russia. Roskomnadzor, the Russian Data Protection regulator, has commenced enforcement of the law and has already blocked access to one foreign social network, which did not have a physical presence in Russia, but operated a Russian language version of its website.



# EUROPEAN UNION AND EUROPEAN ECONOMIC AREA



The European Union (EU) adopted the General Data Protection Regulation (GDPR) in 2016, which is binding on all EU member states, as well as members of the European Economic Area (EEA). The GDPR will become enforceable as of May 25, 2018. On that date, Directive 95/46/EC on the Protection of Personal Data, which had been the legal basis of the provisions of the national data protection laws of all EU and EEA member states, will be repealed.

The other important document governing aspects of the protection of personal data in the EU/EEA is Directive 2002/58/EC on Privacy and Electronic Communications. This directive is being phased out and a first draft of an E-Privacy Regulation, which would replace it, has been published and could enter into effect as of May 25, 2018, but delays are likely.

From a security standpoint, the Network Information Security Directive (NIS Directive) is paving the way to more stringent security requirements. Adopted in 2016, the NIS Directive requires EU/EEA member states to implement new information security laws for the protection of critical infrastructure and essential services by May 2018. Cloud service providers and some cloud users are likely to be affected by the national laws that will implement the overarching NIS Directive.

## **General Data Protection Regulation (GDPR)**

The new GDPR is directly binding on any corporation that processes the data of EU citizens, and will be adjudicated by the data supervisory authorities or the courts of the member states that have the closest relationship with the individuals or the entities on both sides of the dispute.

*Applicability:* The GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or processor in the EU/EEA, regardless of whether the processing takes place in the EU/EEA or not. It also applies to the processing of personal data of data subjects who are in the EU/EEA by a controller or a processor not established in the EU/EEA if the processing relates to (a) the offering of goods or services irrespective of whether a payment by the data subject is required; or (b) the monitoring of the behavior of a data subject, when the behavior takes place within the EU/EEA.

*Lawfulness:* The processing of personal data is allowed only if (a) the data subject has freely given specific, informed and unambiguous indication of his/her consent to the processing of his/her personal data, or (b) the processing is authorized by a statutory provision.

*Accountability Obligations:* The GDPR has created numerous obligations for companies. For example,



the GDPR requires companies to keep records of their data processing activities. Certain categories of processing require a prior "Privacy Impact Assessment." Companies are expected to develop and operate their products and services in accordance with "privacy by design" and "privacy by default" principles.

*Data Subjects' Rights:* Data subjects have rights to information regarding the processing of their data: the right to object to certain uses of their personal data; to have their data corrected or erased; to be compensated for damages suffered as a result of unlawful processing; the right to be forgotten; and the right to data portability. The existence of these rights significantly affects cloud service relationships.

*Cross-border Data Transfer Restrictions:* The transfer of personal data outside the EU/EEA to a country that does not offer a similar range of protection of personal data and privacy rights is prohibited. To prove that it will be offering the "adequate level of protection" required, a company may use one of several methods, such as executing Standard Contractual Clauses (SCC), signing up to the EU-US Privacy Shield, obtaining certification of Binding Corporate Rules (BCRs), or complying with an approved industry Code of Conduct or approved certification mechanism. In rare cases, the transfer might be effected with the explicit, informed, consent of the data subject, or if other exceptions apply.

*Breaches of Security:* The GDPR requires companies to report that they have suffered a breach of security. The reporting requirements are risk-based, and there are different requirements for reporting the breach to the Supervisory Authority and to the affected data subjects. Breaches must be reported within 72 hours of the company becoming aware of the incident.

*Discrepancies among Member States:* There are numerous instances where each member state may adopt its own rules. For example, Germany requires that a Data Protection Officer be appointed if the company has more than nine employees.

*Sanctions:* Violations of the GDPR expose a company to significant sanctions. These sanctions may reach up to the greater of four percent of their global turnover or gross income, or up to EUR 20 million.

### **Network Information Security Directive (NIS Directive)**

The NIS Directive entered into force in August 2016, requiring each EU/EEA member state to implement the Directive into its national legislation by May 2018. The NIS Directive establishes a framework to enable networks and information systems to resist, at a given level of confidence, actions that compromise the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data, or the related services that are offered by or accessible through those networks and information systems.

The NIS Directive requires that member state's national laws impose network and information security requirements on operators of essential services, i.e., entities that provide a service essential for the maintenance of critical societal and/or economic activities; and where an incident to the network and information systems of that service would have significant disruptive effects on the provision of that service. The requirements to be implemented into national laws include the following:

- Taking technical and organizational measures to manage risks posed to the security of networks and information systems used in their operations;
- Taking appropriate measures to prevent and minimize the impact of incidents affecting the security of the networks and information systems used for the provision of such essential services, to facilitate the continuation of those services;
- Notifying, without undue delay, the competent authorities or agencies of incidents having a significant impact on the continuity of the essential services they provide;
- Providing information necessary to assess the security of their networks and information systems
- Providing evidence of the effective implementation of security policies, such as the results of a security audit.

The NIS Directive also requires that member state's national laws impose network and information security requirements on digital service providers, such as online market places (e.g., e-commerce platforms), cloud computing services; and online search engines. Digital service providers based outside the EU that provide services within the EU fall under the scope of the NIS Directive.

Member state's national laws will also have to require digital service providers to identify and take appropriate and proportionate technical and organizational measures to manage risks posed to the security of network and information systems they use, such as incident handling, business continuity management, monitoring, auditing and testing, and compliance with international standards.

Member State's national laws will have to require digital service providers to take measures to prevent and minimize the impact of incidents. They will be required to notify the competent authorities or agencies, without undue delay, of any incident having a substantial impact on the provision of a service, including sufficient information to enable the competent authority or agency to determine the significance of any cross-border impact. Where an operator of essential services relies on a third party digital service provider for a service that is essential, the operator will be required to notify any significant impact on the continuity of the essential services due to an incident affecting the digital service provider.

## THE AMERICAS



### Central and South America

Central and South American countries also are adopting data protection laws at a rapid pace. Each of these laws includes a security requirement and places on the data custodian the burden of ensuring the protection and security of personal data wherever the data are located, and especially when transferring to a third party.



For example, Argentina, Chile, Colombia, Mexico, Peru and Uruguay have passed data protection laws inspired mainly by the European directive 95/46/EC, and may include references to the APEC Privacy Framework. The federal data protection law of Mexico includes security breach disclosure provisions.

## North America: United States

Due to its sectoral approach, the United States has hundreds of federal, state and local regulations, from the details of a written information security plan to the rules for disclosing security breaches. As a result, organizations that do business in the United States or collect or process personal or other information of individuals or companies located in the United States are often subject to several federal, state or local privacy or information security laws. The variety and complexity of these rules might be daunting both for providers or users of cloud services and for the service providers and subcontractors who participate in the provision of these services.

### ***U.S. Federal Laws***

Numerous federal laws and their related regulations—such as the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Children's Online Privacy Protection Act of 1998 (COPPA)—contain provisions that pertain to the privacy and the security of personal information. Security-related provisions require companies to adopt reasonable security measures when processing personal data.

Most of these laws require companies to take precautions when hiring subcontractors and service providers. They may also hold organizations responsible for the acts of their subcontractors. For example, the security and privacy rules under GLBA and HIPAA require that covered organizations compel their subcontractors, in written contracts, to use reasonable security measures and comply with data privacy provisions.

### ***U.S. State Laws***

In addition to federal laws and regulations, most U.S. states have laws relating to data privacy and/or data security. These laws apply to any entity that collects or processes personal information (as narrowly defined in the applicable law) of individuals who reside in that state, regardless of where in the United States the data is stored.

Some state laws are elaborate. See, for example, the extensive requirements under Massachusetts' "Standards for the Protection of Personal Information of Residents of the Commonwealth," or 201 CMR 17.00. Other state laws are more general (see Washington State law RCW 19.255.020(2)(b) that assigns liability on the basis of compliance) and a small number of state laws reference other specific standards (such as the Payment Card Industry Data Security Standard, PCI-DSS, mentioned above). Most state laws that address information security issues require that the company have a written contract with the service provider with reasonable security measures. Numerous state laws also require companies to provide adequate privacy protections and security for personal data, and require their service providers to do the same.

### ***Security Breach Disclosure Laws***

Numerous federal security laws or rules, such as those applying to healthcare providers, as well as most state laws, require entities that have suffered a breach of security that compromised specified categories of data, such as PHI (patient health information), to promptly notify affected individuals,



and in many cases, state or federal agencies, of the occurrence of the breach of security.

Knowledge and understanding of these laws is critical for both cloud customers and cloud vendors, because breaches of security often trigger significant cost, including for example, the cost of responding to class action suits. Recent breaches of security have been reported to affect hundreds of millions of individuals, and the resulting legal costs and damages to be paid out by affected companies have also been significant.

### ***Federal and State Agencies***

In addition to specific laws and regulations, cloud providers and users should be aware of the “common law of privacy and security,” the nickname given to the body of consent orders that have been published by federal and state government agencies at the conclusion of their investigations into security incidents and events.

For almost 20 years, U.S. government agencies, such as the Federal Trade Commission (FTC) and the State Attorneys General have used their power under Federal or state “unfair and deceptive practices” acts to conduct enforcement actions against companies whose privacy or security practices are inconsistent with claims made in their public disclosures, making their practices unfair or deceptive. The numerous consent decrees issued by the FTC in enforcement cases under **Section 5 of the FTC Act: Unfair or Deceptive Acts or Practices**—or by state attorneys general in similar cases under their states’ unfair and deceptive practices act—at the conclusion of many of these security investigations provide important guidance on the views and objectives of the Federal or State agencies regarding the collection, use and protection of personal information.

### **3.1.2 Contracts and Provider Selection**

Even if a specific activity is not regulated, cloud customers may have a contractual obligation to protect the personal information of their own clients, contacts or employees to insure data is not used for secondary purposes, and is not disclosed to, or shared with, third parties. This obligation may stem, for example, from the Terms and Conditions and Privacy Statement that a company posts on its website, or from contracts that the company has executed with third parties. For example, a data processor may be bound by the terms of its Services Agreement to process personal data only for certain purposes. Alternatively, the company may have entered into contracts (such as service agreements) with its customers, in which it has made specific commitments to protect the data (personal data or company data), limit its use, insure its security, use encryption, etc. The organization must guarantee that, when data in its custody is hosted in the cloud, it will have the continued ability to meet the promises and commitments that it made in its privacy notice(s) or other contracts. Data in the cloud must be used only for the purposes for which it was collected.

If the privacy notice allows individual data subjects to have access to their personal data, and to have this information modified or deleted, the cloud service provider must also allow these access, modification, and deletion rights to be exercised to the same extent as it would in a non-cloud relationship.

When data or operations are transferred to a cloud, the responsibility for protecting and securing the data typically remains with the collector or custodian of that data, even if in some circumstances



this responsibility may be shared with others. Even when it relies on a third party to host or process its data, the custodian of the data remains liable for any loss, damage, or misuse of the data. It is therefore prudent, and may be required by law or regulation, that the data custodian and the cloud provider enter into a formal written agreement that clearly defines the roles, the expectations of the parties, and the allocation of the many responsibilities that are attached to the data at stake. Such an agreement should also clearly identify the permitted and prohibited uses of the data, and the measures to be taken if the data were stolen or compromised.

The laws, regulations, standards and the related best practices discussed above also require data custodians to ensure that these obligations will be fulfilled by conducting due diligence (before execution of the contract) or security audits (during performance of the contract).

### 3.1.2.1 Internal Due Diligence

Companies are the custodians of data entrusted to them. As seen above, numerous laws, regulations and contracts prohibit, restrict and limit disclosure and transfer of data to a third party. For example, health information protected under HIPAA cannot be transferred to a third party or "business associate" without imposing specific obligations on that associate. In addition, if data originates abroad, it is likely that there are significant obstacles to its transfer across borders into a country that does not provide "adequate protection" to privacy rights and personal data.

Before entering into a cloud computing arrangement, both the cloud service vendor and the cloud customer should evaluate respective practices, needs and restrictions to identify relevant legal barriers and compliance requirements. For example, a cloud customer should determine whether its business model allows for the use of cloud computing services, and under which conditions. The nature of its business might be such that it is restricted by law from relinquishing control of company data. A cloud vendor may find it prudent to evaluate in advance the cost of doing business in certain markets that might be subject to legal requirements with which the vendor is unfamiliar.

A cloud customer should investigate whether it has entered into any confidentiality agreements or data use agreements that might restrict the transfer of data to third parties, even if these third parties are service providers. If the company, or potential cloud customer, has signed a confidentiality agreement to protect personal information or trade secrets, this agreement probably prohibits hiring a subcontractor without prior permission of the data owner. A data use agreement to which the company is a party may require the consent of a customer if the company plans to subcontract the processing of the customer's data to a third party. That restriction would in most cases apply to transfers to a cloud service provider. Under these circumstances, moving data to a cloud without the prior permission of the customer (data owner) would cause a breach in the data use agreement with that customer.

In other circumstances, the data processed by the company might be so sensitive or confidential that it should not be transferred to a cloud service, or the transfer might require significant precautions. This might be the case, for example, for files that pertain to high stakes projects such as R&D road maps, or plans for an upcoming IPO, merger or acquisition.



### 3.1.2.2 Monitoring, Testing, and Updating

The cloud environment is not static. It evolves and involved parties must adapt. Periodic monitoring, testing, and evaluation of cloud services are recommended in order to insure required privacy and security measures are followed. Without periodic testing of cloud services, control efficacy may be compromised in an undetected fashion.

In addition, the legal, regulatory, and technical landscape in which any company operates changes at a rapid pace. New security threats, new laws, and new compliance requirements must be addressed promptly. Both cloud clients and cloud providers must keep abreast of relevant legal, regulatory, contractual, and other requirements, and ensure that both their operations remain compliant with applicable laws and regulations, and that the security measures in place continue to evolve as new technologies emerge.

### 3.1.2.3 External Due Diligence

Before entering into any contract, a critical part of due diligence must be to request and review all relevant aspects of the operations of the other party—in this case, that of the proposed cloud provider or vendor. A purchaser of cloud services needs to ensure that it understands the particular application or service it is contemplating acquiring. The extent of the due diligence and the time invested in it will depend upon the circumstances. The process may take a day, a week or a month depending on the specific needs of the customer, the nature of the data to be processed, the sensitivity and intensity of the processing, and other factors that would make a particular operation routine or highly sensitive.

Thus, depending on the nature of the proposed project, the due diligence may involve evaluating the nature and completeness of the services provided, the reputation for quality or stability of the service, the availability of a certain level of support or maintenance, the responsiveness of customer service, the speed of the network, and the location of the data centers. Interviewing customers may provide valuable insight. Reviewing reports of litigation filed against cloud providers and conducting online searches to evaluate a vendor's reputation may also be eye-opening.

In most cases, the cloud customer will want to evaluate at least the applicable service level, end-user and legal agreements; privacy policies; security disclosures; and proof of compliance with applicable legal requirements (e.g., registration requirements) to ensure the conditions stated by the cloud provider are suitable for the customer's organization. Depending on the expected depth and intensity of the due diligence, issues to be investigated may include the following:

- Will the service be reliable and easy to use?
- How will the servers be used to process data?
- How will the service operate and be provided?
- Will data be collocated with other customers' data?
- How will data be protected from intrusion or disasters?
- How will the price evolve over time?
- Will the cloud vendor meet the company's computing and access needs?
- Will the cloud vendor remain in business for the next few years? What is its financial profile?
- What service levels will be offered?

- What security measures are used?
- What will happen in the event of a security breach?

Reviewing all terms and conditions of the cloud services agreement (including all annexes, schedules and appendices) is good due diligence for any new project. It is especially critical for cloud computing, as some vendor terms and conditions will be non-negotiable. In those instances, the customer needs to make an informed decision to use or not use a provider.

#### **3.1.2.4 Contract Negotiations**

Cloud contracts are intended to accurately describe the understanding of all parties. Numerous precautions and measures can be taken by the parties to reduce exposure to legal, commercial and reputational risk in connection with the use of cloud services.

The proposed contact should always be reviewed carefully, even if one is told that it is not negotiable. For one thing, it might actually be possible to negotiate changes. Even if it is not possible to do so, each purchaser of cloud services should understand the consequences and implications of the engagement it is making. A contract that cannot be negotiated is likely to lack some of the protections that the typical customer would need. In this case, the customer should weigh the risks from foregoing these protections against potential benefits.

#### **3.1.2.5 Reliance on Third-Party Audits and Attestations**

Audits and compliance are covered in more detail in Domain 4, but two considerations may affect contractual and legal/regulatory requirements. In cloud computing, third-party audits and attestations are frequently used to assure compliance with aspects of the cloud provider's infrastructure, allowing a customer to build their own compliant services on top of the cloud platform. It is critical for a provider to publish, and a customer to evaluate, the scope of the assessment, and which features and services are included in the assessment.

For example, a cloud provider's newest storage offering may not be HIPAA-compliant (and thus the provider may not be willing to sign a HIPAA Business Associate Agreement (BAA) covering it), even though many of its other service offerings are able to be used in a HIPAA-compliant fashion.

### **3.1.3 Electronic Discovery**

U.S. rules around "discovery"—the process by which an opposing party obtains private documents for use in litigation—cover a wide range of potential documents. In particular, discovery need not be limited to documents known at the outset to be admissible as evidence in court; instead, discovery will apply to all documents reasonably calculated to lead to admissible evidence (evidence that is both relevant and probative). See [Rule 26, Federal Rules of Civil Procedure](#) (FRCP).

In recent years, many litigants have deleted, lost or modified evidence that was detrimental to their case. In these cases, the Federal Rules of Civil Procedure allow, among other penalties, money to be awarded to the side not responsible for the destruction; in some cases, the jury may be given



an instruction on an “adverse inference” (where a jury is instructed to assume that the destroyed evidence contains the worst possible information for the party that destroyed it). See Rule 37, FRCP. As a result of the ongoing litigation in this area, the FRCP have been changed to clarify the obligations of the parties, especially in the case of electronically stored information (ESI).

Since the cloud will become the repository of most ESI needed in litigation or an investigation, cloud service providers and their clients must carefully plan how they will be able to identify all documents that pertain to a case, in order to be able to fulfill the stringent requirements imposed by FRCP 26 with regard to ESI, and the state equivalents to these laws. In this regard, the cloud service client and provider need to consider the following issues in matters when a client is subject to a discovery request and potentially relevant data exists with the cloud provider.

### **3.1.3.1 Possession, Custody and Control**

In most jurisdictions in the United States, a party’s obligation to produce relevant information is limited to documents and data within its possession, custody or control. Hosting relevant data via a third party, such as a cloud provider, generally does not obviate a party’s obligation to produce information. However, not all data hosted by a cloud provider may be in the control of a client (e.g., disaster recovery systems, or certain metadata created and maintained by the cloud provider to operate its environment). Distinguishing the data that is and is not available to the client may be in the interest of both the client and provider at the outset of a relationship. The obligations of the cloud service provider as cloud data handler with regard to the production of information in response to legal process is an issue left to each jurisdiction to resolve.

### **3.1.3.2 Relevant Cloud Applications and Environment**

On occasion, an actual cloud application or environment could itself be relevant to resolving a dispute. In these circumstances, the application and environment will likely be outside the control of the client and require that a subpoena or other discovery process be served on the provider directly.

### **3.1.3.3 Searchability and E-Discovery Tools**

In a cloud environment, a client may not be able to apply or use e-discovery tools that it uses in its own environment. Moreover, a client may not have the ability or administrative rights to search or access all the data hosted in the cloud. For example, where a client could access multiple employees’ e-mail accounts on its own server at once, it may not have this ability with e-mail accounts hosted in the cloud. As such, clients need to account for the potential additional time and expense this limited access will cause. To the extent the customer is able to negotiate or supplement the cloud service agreement, this issue could be addressed ahead of time. Otherwise, the cloud customer may have no option other than to address issues on a case-by-case basis; and might therefore have to pay for additional services from the cloud provider.

### **3.1.3.4 Preservation**

Depending on the cloud service and deployment model that a client is using, preservation in the cloud can be similar to preservation in other IT infrastructures, or it can be significantly more complex.



In the United States, a party is generally obligated to undertake reasonable steps to prevent the destruction or modification of data in its possession, custody or control that it knows, or reasonably should know, is relevant either to pending or reasonably anticipated litigation or a government investigation. (This is often referred to as a “litigation hold” on document destruction.) These concerns are addressed broadly by Federal Rule of Civil Procedure 37, though there are myriad jurisdictional rulings that apply to potential litigants. In the European Union, information preservation is governed under Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006. Japan, South Korea and Singapore have similar data protection initiatives. In South America, Brazil and Argentina have the Azeredo Bill and the Argentina Data Retention Law of 2004, Law No. 25.873, respectively.

### 3.1.3.5 Data Retention Laws and Record Keeping Obligations

In addition to data preservation obligations resulting from U.S. laws regarding e-discovery, companies need to be aware that data retention laws require covered entities to retain data for a certain period of time.

**Costs and Storage:** Preservation can require that large volumes of data be retained for extended periods. Customers should consider these questions and determine the risk tolerated before moving to the cloud:

- What are the ramifications of retaining data under the service level agreement (SLA)?
- What happens if the preservation requirements outlast the terms of the SLA?
- If the client preserves the data in place, who pays for the extended storage, and at what cost?
- Does the client have the storage capacity under its SLA?
- Can the client effectively download the data in a forensically sound manner so it can be preserved off-line or near-line?

**Scope of Preservation:** A requesting party is entitled only to data hosted in the cloud that contains, or is reasonably calculated to lead to, relevant, probative information for the legal issue at hand. The party is not entitled to all the data in the cloud or in the application. (The issue of precise limits is likely to be resolved in litigation.) However, if the client does not have the ability to preserve only the relevant information or data in a granular way, it may be required to over-preserve in order to secure reasonable preservation, depending on the investigation. The over-preserved information is then examined for a determination of what must and must not be turned over as part of the discovery process. This process, referred to as a document review or privilege review, may be undertaken by client paid attorney staff or, in some cases, by emerging expert systems. How to sort the ever-more-voluminous quantities of information that may be produced by discovery is an ongoing area of both legal and technical research.

**Dynamic and Shared Storage:** The burden of preserving data in the cloud may be relatively modest if the client has space to hold it in place, if the data is relatively static, and if the people with access are limited and know to preserve the data. However, in a cloud environment that programmatically modifies or purges data, or one where the data is shared with people unaware of the need to preserve, preservation can be more difficult. After a client determines that such data is relevant and needs to be preserved, the client may need to work with the provider to determine a reasonable way to preserve such data.



### 3.1.3.6 Collection

Because of the potential lack of administrative control a client has over its data in the cloud, collection from the cloud can be more difficult, more time-consuming and more expensive than from behind a client's firewall. In particular, a client may not have the same level of visibility across its cloud data, and it may have more difficulty comparing the data it has collected with the data in the cloud to determine that export was reasonably complete and accurate.

*Access and Bandwidth:* In most cases, a client's access to its data in the cloud will be determined by its SLA. This may limit its ability to collect large volumes of data quickly and in a forensically sound manner (i.e., with all reasonably relevant metadata preserved). Clients and cloud providers should consider this issue at the outset of their relationship, and establish a protocol (and cost) for extraordinary access in the case of litigation. Absent these agreements, clients are responsible for the extra time and cost implicated by collection in the cloud when making representations to requesting parties and courts. Note that FRCP 26(b)(2)(B) excuses a litigant who is able to show that the information requested is not reasonably accessible.

However, a court may nonetheless order discovery from such sources if the requesting party is able to show why this information is needed and may not be obtained otherwise.

In a related issue, a client's right of access may provide them access to a full range of data, but not provide them the degree of functionality that would best assist them in a given situation. For example, a client may have access to three years of retail transactional data, but may only be able to download data two weeks at a time because of functionality constraints. Moreover, a client may not only have view of limited metadata. It is prudent for a client to learn what is possible with the tools available before it becomes necessary to use them as a part of active litigation.

*Forensics:* Bit-by-bit imaging of a cloud data source is generally difficult or impossible. For obvious security reasons, providers are reluctant to allow access to their hardware, particularly in a multi-tenant environment where a client could gain access to other clients' data. Even in a private cloud, forensics may be extremely difficult, and clients may need to notify opposing counsel or the courts of these limitations. (Again, FRCP 26(b)(2)(B) may provide relief from such undue burdens.) Luckily, this type of forensic analysis is rarely warranted in cloud computing, because the environment often consists of a structured data hierarchy or virtualization that does not provide significant additional relevant information in a bit-by-bit analysis.

*Reasonable Integrity:* A client subject to a discovery request should undertake reasonable steps to validate that its collection from its cloud provider is complete and accurate, especially where ordinary business procedures for the request are unavailable and litigation-specific measures are being used to obtain the information. This process is separate from verifying that the data stored in the cloud is accurate, authenticated or admissible.

*Limits to Accessibility:* Due to differences in how data is stored, and the access rights and privileges available to the owner of the data, there are cases where a cloud customer may not be able to access all their data stored in a cloud. The cloud customer and cloud provider may have to analyze the request for information and the pertinent data structures for relevance, materiality,



proportionality, or accessibility, when responding to a discovery request.

### 3.1.3.7 Direct Access

Outside the cloud environment, a requesting party's direct access to a responding party's IT environment is not generally favored. (It does happen from time to time. In fact, some courts have been willing to allow no-notice seizures of IT equipment for the purpose of evidence preservation in civil cases, including employment disputes.) In the cloud environment, it is even less favored and may be impossible as a forensic analysis may be impossible. Some cloud providers may not be able to provide direct access, because the hardware and facilities are outside its possession, custody or control, and a requesting party would need to negotiate directly with the provider for such access.

### 3.1.3.8 Native Production

Cloud service providers often store data in highly proprietary systems and applications that clients do not control. Generally, ESI is expected to be produced in standard formats (such as PDF for electronic documents), unless information lost by conversion (such as metadata) is relevant to the dispute. Data in its cloud-native format may be useless to the requesting party. In these circumstances, it may be best for all concerned—requesting party, producing party and provider—that the relevant information be exported using standard protocols within the cloud environment, with due care given to preserving relevant information.

### 3.1.3.9 Authentication

Authentication in this context refers to forensic authentication of data admitted into evidence. (This should not be confused with user authentication, which is a component of Identity Management.) Storing data in the cloud does not affect the authentication of data to determine if it should be admitted into evidence. The question is whether the document is what it purports to be. For example, an e-mail is no more or less authentic because it was stored behind a company's firewall or was stored in the cloud; the question is whether it was stored with integrity, such that the court can trust that it has not been altered since it was created. Absent other evidence, such as tampering or hacking, documents should not be considered more or less admissible or credible merely because they were created or stored in the cloud.

### 3.1.3.10 Cooperation Between Provider and Client in E-Discovery

It is in the best interests of both providers and clients to consider the complications caused by discovery at the beginning of their relationship and to account for it in their SLAs. Providers may want to consider designing their cloud offerings to include discovery services to attract clients ("Discovery by Design"). In any event, clients and providers should consider including an agreement to reasonably cooperate with each other in the event of discovery requests against either.

### 3.1.3.11 Response to a Subpoena or Search Warrant

Should a cloud service provider receive, from a third party, a request to provide information; this may be in the form of a subpoena, a warrant, or a court order in which access to the client data is



demanded. The client may want to have the ability to fight the request for access in order to protect the confidentiality of their data. To this end, the cloud service agreement should require the cloud service provider to notify the customer that a subpoena was received and give the company time to fight the request for access.

The cloud service provider might be tempted to reply to the request by opening its facilities and providing the requester with whatever they request. Before doing so, the cloud service provider should ensure, in consultation with counsel, that the request is legal and solid. The cloud service provider should carefully analyze the request before disclosing information in its custody, and consider whether it can meet its obligations to its clients when releasing information. In some cases, a provider may be better able to serve the needs of its clients by fighting an overbroad or otherwise problematic demand for information.

### 3.1.3.12 More Information

For more reading on discovery and electronically stored information, there are a wide variety of sources. One that may be of interest is the Sedona Conference, a nonprofit, research and educational institute that has for several years made influential recommendations about the handling of ESI, which have in turn shaped this emerging area of law. Note, however, that their recommendations do not themselves carry the force of law.

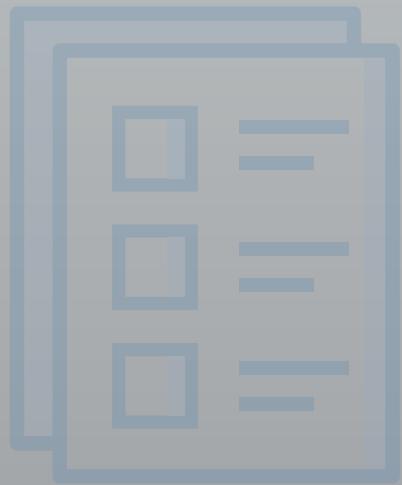
## 3.2 Recommendations

- Cloud customers should understand the relevant legal and regulatory frameworks, as well as contractual requirements and restrictions that apply to the handling of their data or data in their custody, and the conduct of their operations, before moving systems and data to the cloud.
- Cloud providers should clearly and conspicuously disclose their policies, requirements and capabilities, including all terms and conditions that apply to the services they provide.
- Cloud customers should conduct a comprehensive evaluation of a proposed cloud service provider before signing a contract, and should regularly update this evaluation and monitor the scope, nature and consistency of the services they purchase.
- Cloud providers should publish their policies, requirements and capabilities to meet legal obligations for customers, such as electronic discovery.
- Cloud customers should understand the legal implications of using particular cloud providers and match those to their legal requirements.
- Cloud customers should understand the legal implications of where the cloud provider physically operates and stores information.
- Cloud customer should decide whether to choose where their data will be hosted, if the option is available, to comply with their own jurisdictional requirements.
- Cloud customers and providers should have a clear understanding of the legal and technical requirements to meet any electronic discovery requests.
- Cloud customers should understand that click-through legal agreements to use a cloud service do not negate requirements for a provider to perform due diligence.



# DOMAIN 4

# Compliance and Audit Management



## 4.0 Introduction

Organizations face new challenges as they migrate from traditional data centers to the cloud. Delivering, measuring, and communicating compliance with a multitude of regulations across multiple jurisdictions are among the largest of these challenges. Customers and providers alike need to understand and appreciate the jurisdictional differences and their implications on existing compliance and audit standards, processes, and practices. The distributed and virtualized nature of cloud computing requires significant adjustment from approaches based on definite and physical instantiations of information and processes.

In addition to providers and customers, regulators and auditors are also adjusting to the new world of cloud computing. Few existing regulations were written to account for virtualized environments or cloud deployments. A cloud user can be challenged to show auditors that the organization is in compliance. Understanding the interaction of cloud computing and the regulatory environment is a key component of any cloud strategy. Cloud customers, auditors, and providers must consider and understand the following:

- Regulatory implications for using a particular cloud service or provider, giving particular attention to any cross-border or multi-jurisdictional issues when applicable.
- Assignment of compliance responsibilities between the provider and customer, including indirect providers (i.e., the cloud provider of your cloud provider). This includes the concept of compliance inheritance where a provider may have parts of their service certified as compliant which removes this from the audit scope of the customer, but the customer is still responsible for the compliance of everything they build on top of the provider.
- Provider capabilities for demonstrating compliance, including document generation, evidence production, and process compliance, in a timely manner.

Some additional cloud-specific issues to pay particular attention to include:

- The role of provider audits and certifications and how those affect customer audit (or assessment) scope.
- Understanding which features and services of a cloud provider are within the scope of which



audits and assessments.

- Managing compliance and audits over time.
- Working with regulators and auditors who may lack experience with cloud computing technology.
- Working with providers who may lack audit and or regulatory compliance experience.

## 4.1 Overview

Achieving and maintaining compliance with a plethora of modern regulations and standards is a core activity for most information security teams and a critical tool of governance and risk management. So much so that the tools and teams in this realm have their own acronym: GRC, for governance, risk, and compliance. Although very closely related with audits — which are a key mechanism to support, assure, and demonstrate compliance — there is more to compliance than audits and more to audits than using them to assure regulatory compliance. For our purposes:

- Compliance validates awareness of and adherence to corporate obligations (e.g., corporate social responsibility, ethics, applicable laws, regulations, contracts, strategies and policies). The compliance process assesses the state of that awareness and adherence, further assessing the risks and potential costs of non-compliance against the costs to achieve compliance, and hence prioritize, fund, and initiate any corrective actions deemed necessary.
- Audits are a key tool for proving (or disproving) compliance. We also use audits and assessments to support non-compliance risk decisions.

This section discusses these interrelated domains individually to better focus on the implications cloud computing has on each.

### 4.1.1 Compliance

Information technology in the cloud (or anywhere really) is increasingly subject to a plethora of policies and regulations from governments, industry groups, business relationships, and other stakeholders. Compliance management is a tool of governance; it is how an organization assesses, remediates, and proves it is meeting these internal and external obligations.

Regulations, in particular, typically have strong implications for information technology and its governance, especially in terms of monitoring, management, protection, and disclosure. Many regulations and obligations require a certain level of security, which is why information security is so deeply coupled with compliance. Security controls are thus an important tool to assure compliance, and evaluation and testing of these controls is a core activity for security professionals. This includes assessments even when performed by dedicated internal or external auditors.

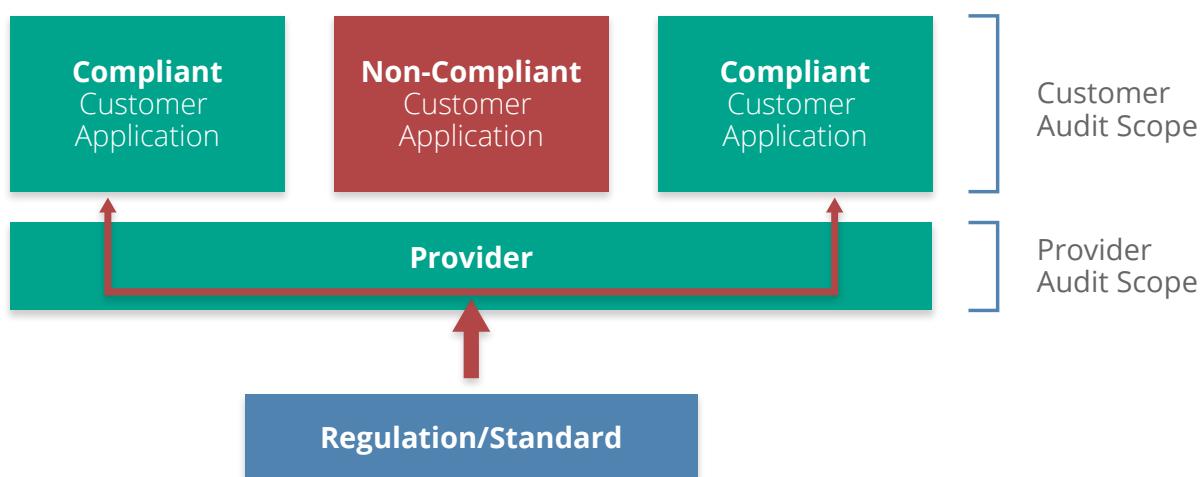
#### **4.1.1.1 How Cloud Changes Compliance**

As with security, compliance in the cloud is a shared responsibility model. Both the cloud provider and customer have responsibilities, but the customer is *always ultimately responsible for their own compliance*. These responsibilities are defined through contracts, audits/assessments, and specifics of the compliance requirements.

Cloud customers, particularly in public cloud, must rely more on third-party attestations of the provider to understand their compliance alignment and gaps. Since public cloud providers rely on economies of scale to manage costs they often will not allow customers to perform their own audits. Instead, similar to financial audits of public companies, they engage with a third-party firm to perform audits and issue attestations. Thus the cloud customer doesn't typically get to define the scope or perform the audit themselves. They will instead need to rely on these reports and attestations to determine if the service meets their compliance obligations.

Many cloud providers are certified for various regulations and industry requirements, such as PCI DSS, SOC1, SOC2, HIPAA, best practices/frameworks like CSA CCM, and global/regional regulations like the EU GDPR. These are sometimes referred to as *pass-through audits*. A pass-through audit is a form of *compliance inheritance*. In this model all or some of the cloud provider's infrastructure and services undergo an audit to a compliance standard. The provider takes responsibility for the costs and maintenance of these certifications. Provider audits, including pass-through audits, need to be understood within their limitations:

- They certify that the *provider* is compliant.
- It is still the responsibility of the customer to *build compliant applications and services on the cloud*.
- This means the provider's infrastructure/services are not within scope of a customer's audit/assessment. But everything the customer builds themselves is still within scope.
- The customer is still ultimately responsible for maintaining the compliance of what they build and manage. For example, if an IaaS provider is PCI DSS-certified, the customer can build their own PCI-compliant service on that platform and the provider's infrastructure and operations should be outside the *customer's* assessment scope. However, the customer can just as easily run afoul of PCI and fail their assessment if they don't design their own application running in the cloud properly.



*With compliance inheritance the cloud provider's infrastructure is out of scope for a customer's compliance audit, but everything the customer configures and builds on top of the certified services is still within scope.*



Cloud compliance issues aren't merely limited to pass-through audits; the nature of cloud also creates additional differentiators.

Many cloud providers offer globally distributed data centers running off a central management console/platform. It is still the customer's responsibility to manage and understand where to deploy data and services and still maintain their legal compliance across national and international jurisdictions.

Organizations have the same responsibility in traditional computing, but the cloud dramatically reduces the friction of these potentially international deployments, e.g., a developer can potentially deploy regulated data in a non-compliant country without having to request an international data center and sign off on multiple levels of contracts, should the proper controls not be enabled to prevent this.

Not all features and services within a given cloud provider are necessarily compliant and certified/audited with respect to all regulations and standards. It is incumbent on the cloud provider to communicate certifications and attestations clearly, and for customers to understand the scopes and limitations.

### **4.1.2 Audit Management**

Proper organizational governance naturally includes audit and assurance. Audits must be independently conducted and should be robustly designed to reflect best practice, appropriate resources, and tested protocols and standards. Before delving into cloud implications we need to define the scope of audit management related to information security.

Audits and assessments are mechanisms to document compliance with internal or external requirements (or identify deficiencies). Reporting needs to include a compliance determination, as well as a list of identified issues, risks, and remediation recommendations. Audits and assessments aren't limited to information security, but those related to information security typically focus on evaluating the effectiveness of security management and controls. Most organizations are subject to a mix of internal and external audits and assessments to assure compliance with internal and external requirements.

All audits have variable scope and statement of applicability, which defines what is evaluated (e.g., all systems with financial data) and to which controls (e.g., an industry standard, custom scope, or both). An attestation is a legal statement from a third party, which can be used as their statement of audit findings. Attestations are a key tool when evaluating and working with cloud providers since the cloud customer does not always get to perform their own assessments.

Audit management includes the management of all activities related to audits and assessments, such as determining requirements, scope, scheduling, and responsibilities.

#### **4.1.2.1 How Cloud Changes Audit Management**

Some cloud customers may be used to auditing third-party providers, but the nature of cloud computing and contracts with cloud providers will often preclude things like on-premises audits. Customers should understand that providers can (and often should) consider on-premises audits a



security risk when providing multitenant services. Multiple on-premises audits from large numbers of customers present clear logistical and security challenges, especially when the provider relies on shared assets to create the resource pools.

Customers working with these providers will have to rely more on third-party attestations rather than audits they perform themselves. Depending on the audit standard, actual results may only be releasable under a nondisclosure agreement (NDA), which means customers will need to enter into a basic legal agreement before gaining access to attestations for risk assessments or other evaluative purposes. This is often due to legal or contractual requirements with the audit firm, not due to any attempts and obfuscation by the cloud provider.

Cloud providers should understand that customers still need assurance that the provider meets their contractual and regulatory obligations, and should thus provide rigorous third-party attestations to prove they meet their obligations, especially when the provider does not allow direct customer assessments. These should be based on industry standards, with clearly defined scopes and the list of specific controls evaluated. Publishing certifications and attestations (to the degree legally allowed) will greatly assist cloud customers in evaluating providers. The Cloud Security Alliance STAR Registry offers a central repository for providers to publicly release these documents.

Some standards, such as SSAE 16, attest that documented controls work as designed/required. The standard doesn't necessarily define the *scope of controls*, so both are needed to perform a full evaluation. Also, attestations and certifications don't necessarily apply equally to all services offered by a cloud provider. Providers should be clear about which services and features are covered, and it is the responsibility of the customer to pay attention and understand the implications on their use of the provider.

Certain types of customer technical assessments and audits (such as a vulnerability assessment) may be limited in the provider's terms of service, and may require permission. This is often to help the provider distinguish between a legitimate assessment and an attack.

It's important to remember that attestations and certifications are point-in-time activities. An attestation is a statement of an "over a period of time" assessment and may not be valid at any future point. Providers must keep any published results current or they risk exposing their customers to risks of non-compliance. Depending on contracts, this could even lead to legal exposures to the provider. Customers are also responsible for ensuring they rely on current results and track when their providers' statuses change over time.

*Artifacts* are the logs, documentation, and other materials needed for audits and compliance; they are the evidence to support compliance activities. Both providers and customers have responsibilities for producing and managing their respective artifacts.

### Audit Logs

### Activity Reporting

### System Configuration Details

### Change Management Details

*Collecting and maintaining artifacts of compliance will change when using a cloud provider.*



Customers are ultimately responsible for the artifacts to support their own audits, and thus need to know what the provider offers, and create their own artifacts to cover any gaps. For example, by building more robust logging into an application since server logs on PaaS may not be available.

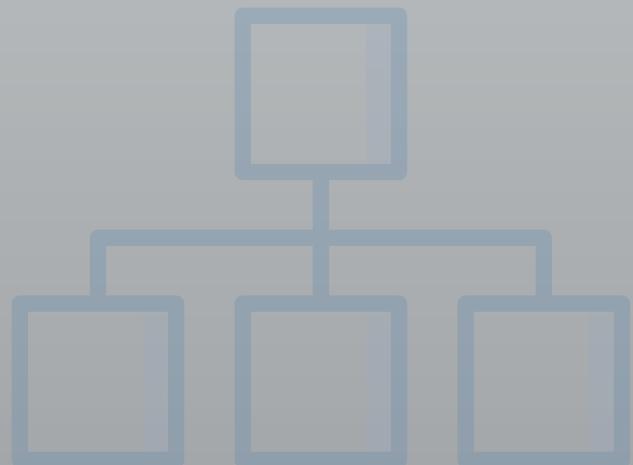
## 4.2 Recommendations

- Compliance, audit, and assurance should be continuous. They should not be seen as merely point-in-time activities, and many standards and regulations are moving more towards this model. This is especially true in cloud computing, where both the provider and customer tend to be in more-constant flux and are rarely ever in a static state.
- Cloud providers should:
  - Clearly communicate their audit results, certifications, and attestations with particular attention to:
    - The scope of assessments.
    - Which specific features/services are covered in which locations and jurisdictions.
    - How customers can deploy compliant applications and services in the cloud.
    - Any additional customer responsibilities and limitations.
  - Cloud providers must maintain their certifications/attestations over time and proactively communicate any changes in status.
  - Cloud providers should engage in continuous compliance initiatives to avoid creating any gaps, and thus exposures, for their customers.
  - Provide customers commonly needed evidence and artifacts of compliance, such as logs of administrative activity the customer cannot otherwise collect on their own.
- Cloud customers should:
  - Understand their full compliance obligations before deploying, migrating to, or developing in the cloud.
  - Evaluate a provider's third-party attestations and certifications and align those to compliance needs.
  - Understand the scope of assessments and certifications, including both the controls and the features/services covered.
  - Attempt to select auditors with experience in cloud computing, especially if pass-through audits and certifications will be used to manage the customer's audit scope.
  - Ensure they understand what artifacts of compliance the provider offers, and effectively collect and manage those artifacts.
    - Create and collect their own artifacts when the provider's artifacts are not sufficient.
  - Keep a register of cloud providers used, relevant compliance requirements, and current status. The Cloud Security Alliance Cloud Controls Matrix can support this activity.



# DOMAIN 5

# Information Governance



## 5.0 Introduction

The primary goal of information security is to protect the fundamental data that powers our systems and applications. As companies transition to cloud computing, the traditional methods of securing data are challenged by cloud-based architectures. Elasticity, multi-tenancy, new physical and logical architectures, and abstracted controls require new data security strategies. In many cloud deployments, users even transfer data to external — or even public — environments in ways that would have been unthinkable only a few years ago.

Managing information in the era of cloud computing is a daunting challenge that affects all organizations and requires not merely new technical protections but new approaches to fundamental governance. Although cloud computing has at least some effect on all areas of information governance, it particularly impacts compliance, privacy, and corporate policies due to the increased complexity in working with third parties and managing jurisdictional boundaries.

Definition of information/data governance:

*Ensuring the use of data and information complies with organizational policies, standards and strategy — including regulatory, contractual, and business objectives.*

Our data is always subject to a range of requirements: some placed on us by others — like regulatory agencies or customers and partners — others that are self-defined based on our risk tolerance or simply how we want to manage operations. Information governance includes the corporate structures and controls we use to ensure we handle data in accordance with our goals and requirements.

There are numerous aspects of having data stored in the cloud that have an impact on information and data governance requirements.

- *Multitenancy:* Multitenancy presents complicated security implications. When data is stored in the public cloud, it's stored on shared infrastructure with other, untrusted tenants. Even in a private cloud environment, it is stored and managed on infrastructure that's shared across different business units, which likely have different governance needs.

- *Shared security responsibility:* With greater sharing of environments comes greater shared security responsibilities. Data is now more likely to be owned and managed by different teams or even organizations. So, it's important to recognize the difference between data custodianship and data ownership.
  - *Ownership*, as the name says, is about who owns the data. It's not always perfectly clear. If a customer provides you data, you might own it or they might still legally own it, depending on law, contracts, and policies. If you host your data on a public cloud provider you should own it, but that might again depend on contracts.
  - *Custodianship* refers to who is managing the data. If a customer gives you their personal information and you don't have the rights to own it, you are merely the custodian. That means you can only use it in approved ways. If you use a public cloud provider, they, likewise, become the custodian of the data, although you likely also have custodial responsibility depending on what controls you implement and manage yourself. Using a provider doesn't obviate your responsibility. Basically, the owner defines the rules (sometimes indirectly through regulation) and the custodian implements the rules. The lines and roles between owner and custodian are impacted by cloud infrastructure, particularly in the case of public cloud.

By hosting customer data in the cloud, we are introducing a third party into the governance model, the cloud provider.

- *Jurisdictional boundaries and data sovereignty:* Since cloud, by definition, enables broad network access, it increases the opportunities to host data in more locations (jurisdictions) and reduces the friction in migrating data. Some providers may not be as transparent about the physical location of the data, while in other cases additional controls may be needed to restrict data to particular locations.
- *Compliance, regulations, and privacy policies:* All of these may be impacted by cloud due to the combination of a third-party provider and jurisdictional changes, e.g., your customer agreement may not allow you to share/use data on a cloud provider, or may have certain security requirements (like encryption).
- *Destruction and removal of data:* This ties in to the technical capabilities of the cloud platform. Can you ensure the destruction and removal of data in accordance with policy?

When migrating to cloud, use it as an opportunity to revisit information architectures. Many of our information architectures today are quite fractured as they were implemented over sometimes decades in the face of ever-changing technologies. Moving to cloud creates a green field opportunity to reexamine how you manage information and find ways to improve things. Don't lift and shift existing problems.

# 5.1 Overview

*Data/information governance* means ensuring that the use of data and information complies with organizational policies, standards, and strategy. This includes regulatory, contractual, and business requirements and objectives. Data is different than information, but we tend to use them interchangeably. Information is data with value. For our purposes, we use both terms to mean the same thing since that is so common.

## 5.1.1 Cloud Information Governance Domains

We will not cover all of data governance, but we'll focus on where hosting in the cloud affects data governance. Cloud computing affects most data governance domains:

- *Information Classification.* This is frequently tied to compliance and affects cloud destinations and handling requirements. Not everyone necessarily has a data classification program, but if you do you need to adjust it for cloud computing.
- *Information Management Policies.* These tie to classification and the cloud needs to be added if you have them. They should also cover the different SPI tiers, since sending data to a SaaS vendor versus building your own IaaS app is very different. You need to determine what is allowed to go where in the cloud? Which products and services? With what security requirements?
- *Location and Jurisdiction Policies.* These have very direct cloud implications. Any outside hosting must comply with locational and jurisdictional requirements. Understand that internal policies can be changed for cloud computing, but legal requirements are hard lines. (See the Legal Domain for more information on this.) Make sure you understand that treaties and laws may create conflicts. You need to work with your legal department when handling regulated data to ensure you comply as best you can.
- *Authorizations.* Cloud computing requires minimal changes to authorizations, but see the data security lifecycle to understand if the cloud impacts.
- *Ownership.* Your organization is always responsible for data and information and that can't be abrogated when moving to the cloud.
- *Custodianship.* Your cloud provider may become custodian. Data hosted but properly encrypted is still under custodianship of the organization.
- *Privacy.* Privacy is a sum of regulatory requirements, contractual obligations, and commitments to customers (e.g. public statements). You need to understand the total requirements and ensure information management and security policies align.
- *Contractual controls.* This is your legal tool for extending governance requirements to a third party, like a cloud provider.
- *Security controls.* Security controls are the tool to implement data governance. They change significantly in cloud computing. See the Data Security and Encryption domain.

## 5.1.2 The Data Security Lifecycle

Although Information Lifecycle Management is a fairly mature field, it doesn't map well to the needs of security professionals. The Data Security Lifecycle is different from Information Lifecycle



Management, reflecting the different needs of the security audience. This is a summary of the lifecycle, and a complete version is available at <http://www.securosis.com/blog/data-security-lifecycle-2.0>. It is simply a tool to help understand the security boundaries and controls around data. It's not meant to be used as a rigorous tool for all types of data. It's a modeling tool to help evaluate data security at a high level and find focus points.

The lifecycle includes six phases from creation to destruction. Although it is shown as a linear progression, once created, data can bounce between phases without restriction, and may not pass through all stages (for example, not all data is eventually destroyed).

*Create.* Creation is the generation of new digital content, or the alteration/updating/modifying of existing content.

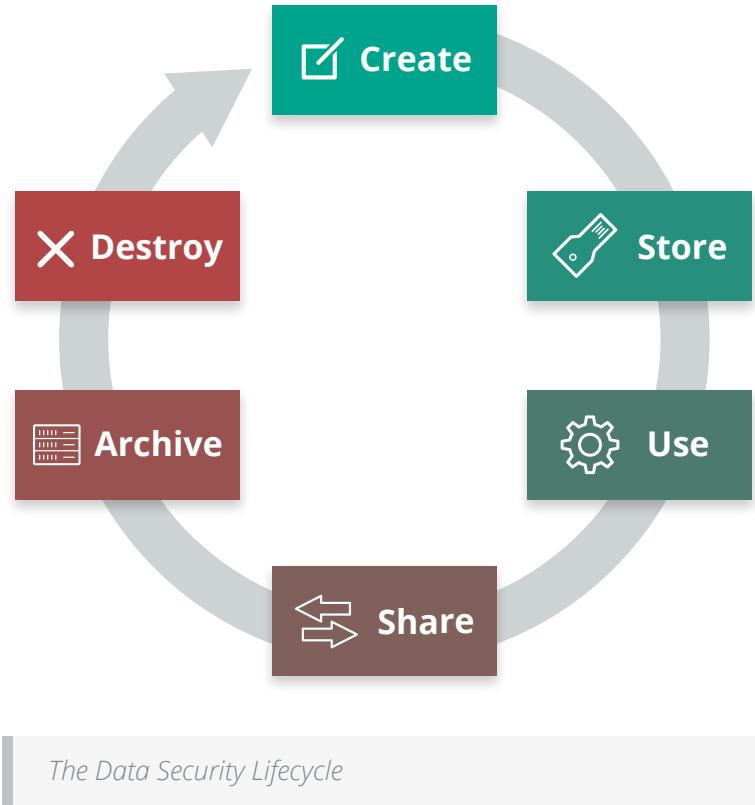
*Store.* Storing is the act committing the digital data to some sort of storage repository and typically occurs nearly simultaneously with creation.

*Use.* Data is viewed, processed, or otherwise used in some sort of activity, not including modification.

*Share.* Information is made accessible to others, such as between users, to customers, and to partners.

*Archive.* Data leaves active use and enters long-term storage.

*Destroy.* Data is permanently destroyed using physical or digital means (e.g., cryptoshredding).

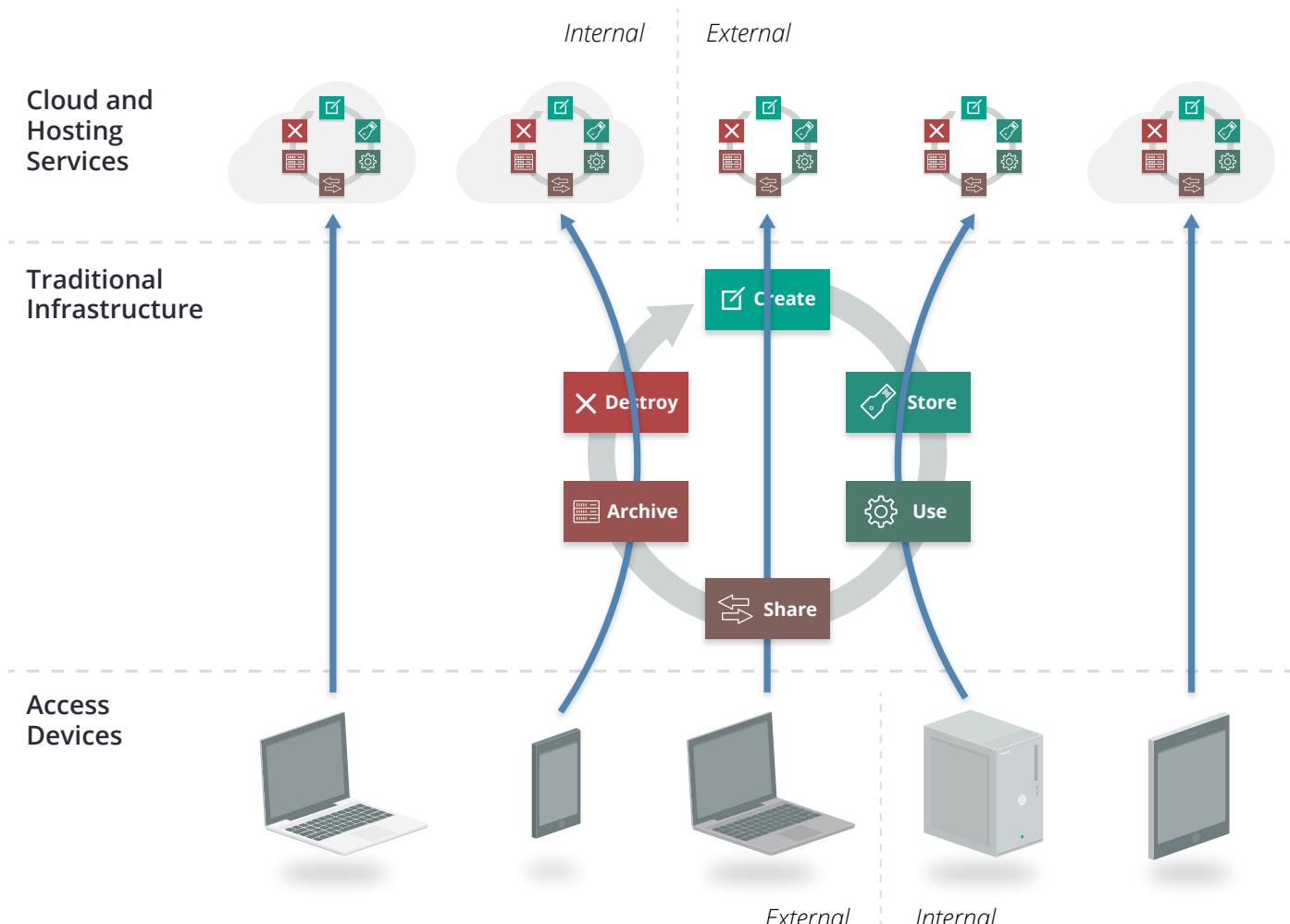


### 5.1.2.1 Locations and Entitlements



The lifecycle represents the phases information passes through but doesn't address its location or how it is accessed.

*Locations:* This can be illustrated by thinking of the lifecycle not as a single, linear operation, but as a series of smaller lifecycles running in different operating environments. At nearly any phase data can move into, out of, and between these environments.



*Data is accessed and stored in multiple locations, each with its own lifecycle.*

Due to all the potential regulatory, contractual, and other jurisdictional issues, it is extremely important to understand both the logical and physical locations of data.

*Entitlements:* When users know where the data lives and how it moves, they need to know who is accessing it and how. There are two factors here:

- Who accesses the data?
- How can they access it (device and channel)?

Data today is accessed using a variety of different devices. These devices have different security characteristics and may use different applications or clients.

### 5.1.2.2 Functions, Actors, and Controls

The next step identifies the functions that can be performed with the data, by a given actor (person or system) and a particular location.

*Functions:* There are three things we can do with a given datum:

- *Read.* View/read the data, including creating, copying, file transfers, dissemination, and other exchanges of information.
- *Process.* Perform a transaction on the data; update it; use it in a business processing transaction, etc.
- *Store.* Hold the data (in a file, database, etc.).

The table below shows which functions map to which phases of the lifecycle:

	Create	Store	Use	Share	Archive	Destroy
Read	X	X	X	X	X	X
Process	X		X			
Store		X			X	

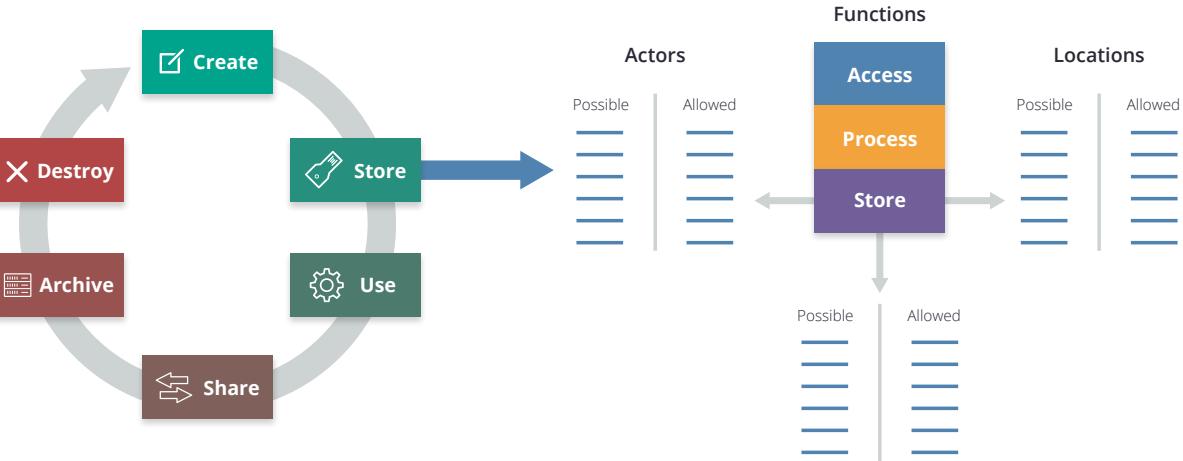
Table 1—Information Lifecycle Phases

An actor (person, application, or system/process, as opposed to the access device) performs each function in a location.

*Controls:* A control restricts a list of possible actions down to allowed actions. The table below shows one way to list the possibilities, which the user then maps to controls.

Function		Action		Location	
Possible	Allowed	Possible	Allowed	Possible	Allowed

Mapping the lifecycle to functions and controls.



*Mapping the lifecycle to functions and controls.*

## 5.2 Recommendations

- Determine your governance requirements for information before planning a transition to cloud. This includes legal and regulatory requirements, contractual obligations and other corporate policies. Your corporate policies and standards may need to be updated to allow a third party to handle data.
- Ensure information governance policies and practices extend to the cloud. This will be done through contractual and security controls.
- When needed, use the data security lifecycle to help model data handling and controls.
- Instead of lifting and shifting existing information architectures take the opportunity of the migration to the cloud to re-think and re-structure what is often the fractured approach used in existing infrastructure. Don't bring bad habits.

# DOMAIN 6

# Management Plane and Business Continuity

## 6.0 Introduction

The management plane is the single most significant security difference between traditional infrastructure and cloud computing. This isn't all of the metastructure (defined in Domain 1) but is the interface to connect with the metastructure and configure much of the cloud.

We always have a management plane, the tools and interfaces we use to manage our infrastructure, platforms, and applications, but cloud abstracts and centralizes administrative management of resources. Instead of controlling a data center configuration with boxes and wires, it is now controlled with API calls and web consoles.

Thus, gaining access to the management plane is like gaining unfettered access to your data center, unless you put the proper security controls in place to limit who can access the management plane and what they can do within it.

To think about it in security terms, the management plane consolidates many things we previously managed through separate systems and tools, and then makes them Internet-accessible with a single set of authentication credentials. This isn't a net loss for security — there are also gains — but it is most definitely different, and it impacts how we need to evaluate and manage security.

Centralization also brings security benefits. There are no hidden resources, you always know where everything you own is at all times, and how it is configured. This is an emergent property of both broad network access and metered service. The cloud controller always needs to know what resources are in the pool, out of the pool, and where they are allocated.

This doesn't mean that all the assets you put into the cloud are equally managed. The cloud controller can't peer into running servers or open up locked files, nor understand the implications of your specific data and information.

In the end, this is an extension of the shared responsibility model discussed in Domain 1 and throughout this Guidance. The cloud management plane is responsible for managing the assets of the resource pool, while the cloud user is responsible for how they configure those assets, and for



the assets they deploy into the cloud.

- The cloud provider is responsible for ensuring the management plane is secure and necessary security features are exposed to the cloud user, such as granular entitlements to control what someone can do even if they have management plane access.
- The cloud user is responsible for properly configuring their use of the management plane, as well as for securing and managing their credentials.

## **6.0.1 Business Continuity and Disaster Recovery in the Cloud**

Business Continuity and Disaster Recovery (BC/DR) is just as important in cloud computing as it is for any other technology. Aside from the differences resulting from the potential involvement of a third-party provider (something we often deal with in BC/DR), there are additional considerations due to the inherent differences when using shared resources.

The three main aspects of BC/DR in the cloud are:

- Ensuring continuity and recovery within a given cloud provider. These are the tools and techniques to best architect your cloud deployment to keep things running if either what you deploy breaks, or a portion of the cloud provider breaks.
- Preparing for and managing cloud provider outages. This extends from the more constrained problems that you can architect around within a provider to the wider outages that take down all or some of the provider in a way that exceeds the capabilities of inherent DR controls.
- Considering options for portability, in case you need to migrate providers or platforms. This could be due to anything from desiring a different feature set to the complete loss of the provider if, for example, they go out of business or you have a legal dispute.

### **6.0.1.1 Architect for Failure**

Cloud platforms can be incredibly resilient, but single cloud assets are typically less resilient than in the case of traditional infrastructure. This is due to the inherently greater fragility of virtualized resources running in highly-complex environments.

This mostly applies to compute, networking, and storage, since those allow closer to raw access, and cloud providers can leverage additional resiliency techniques for their platforms and applications that run on top of IaaS.

However, this means that cloud providers tend to offer options to improve resiliency, often beyond that which is attainable (for equivalent costs) in traditional infrastructure. For example, by enabling multiple “zones,” where you can deploy virtual machines within an auto-scaled group that encompasses physically distinct data centers for high-availability. Your application can be balanced across zones so that if an entire zone goes down your application still stays up. This is quite difficult to implement in a traditional data center, where it typically isn’t cost-effective to build multiple, isolated physical zones across which you can deploy a cross-zone, load-balanced application with automatic failover.



But this extra resiliency is only achievable if you architect to leverage these capabilities. Deploying your application all in one zone, or even on a single virtual machine in a single zone, is likely to be less resilient than deploying on a single, well-maintained physical server.

This is why “lift and shift” wholesale migration of existing applications without architectural changes can reduce resiliency. Existing applications are rarely architected and deployed to work with these resiliency options, yet straight-up virtualization and migration without changes can increase the odds of individual failures.

The ability to manage is higher with IaaS and much lower with SaaS, just like security. For SaaS, you rely on the cloud provider keeping the entire application service up. With IaaS, you can architect your application to account for failures, putting more responsibility in your hands. PaaS, as usual, is in the middle — some PaaS may have resiliency options that you can configure, while other platforms are completely in the hands of the provider.

Overall, a risk-based approach is key:

- Not all assets need equal continuity.
- Don’t drive yourself crazy by planning for full provider outages just because of the perceived loss of control. Look at historical performance.
- Strive to design for RTOs and RPOs equivalent to those on traditional infrastructure.

## 6.1 Overview

### 6.1.1 Management Plane Security

The management plane refers to the interfaces for managing your assets in the cloud. If you deploy virtual machines on a virtual network the management plane is how you launch those machines and configure that network. For SaaS, the management plane is often the “admin” tab of the user interface and where you configure things like users, settings for the organization, etc.

The management plane controls and configures the metastructure (defined in Domain 1), and is also part of the metastructure itself. As a reminder, cloud computing is the act of taking physical assets (like networks and processors) and using them to build resource pools. Metastructure is the glue and guts to create, provision, and deprovision the pools. The management plane includes the interfaces for building and managing the cloud itself, but also the interfaces for cloud users to manage their own allocated resources of the cloud.

The management plane is a key tool for enabling and enforcing separation and isolation in multitenancy. Limiting who can do what with the APIs is one important means for segregating out customers, or different users within a single tenant. Resources are in the pool, out of the pool, and where they are allocated.



### 6.1.1.1 Accessing the Management Plane

APIs and web consoles are the way the management plane is delivered. Application Programming Interfaces allow for programmatic management of the cloud. They are the glue that holds the cloud's components together and enables their orchestration. Since not everyone wants to write programs to manage their cloud, web consoles provide visual interfaces. In many cases web consoles merely use the same APIs you can access directly.

Cloud providers and platforms will also often offer Software Development Kits (SDKs) and Command Line Interfaces (CLIs) to make integrating with their APIs easier.

- *Web consoles* are managed by the provider. They can be organization-specific [typically using Domain Name Server (DNS) redirection tied to federated identity]. For example, when you connect to your cloud file-sharing application you are redirected to your own “version” of the application after you log in. This version will have its own domain name associated with it, which allows you to integrate more easily with federated identity (e.g. instead of all your users logging in to “application.com” they log into “your-organization.application.com”).

As mentioned, most web consoles offer a user interface for the same APIs that you can access directly. Although, depending on the platform or provider’s development process, you may sometimes encounter a mismatch where either a web feature or an API call appear on one before the other.

APIs are typically **REST** for cloud services, since REST is easy to implement across the Internet. REST APIs have become the standard for web-based services since they run over HTTP/S and thus work well across diverse environments.

These can use a variety of authentication mechanisms, as there is no single standard for authentication in REST. HTTP request signing and OAuth are the most common; both of these leverage cryptographic techniques to validate authentication requests.

You still often see services that embed a password in the request. This is less secure and at higher risk for credential exposure. It’s most often seen in older or poorly-designed web platforms that built their web interface first and only added consumer APIs later. If you do encounter this, you need to use dedicated accounts for API access if possible, in order to reduce the opportunities for credential exposure.

### 6.1.1.2 Securing the Management Plane

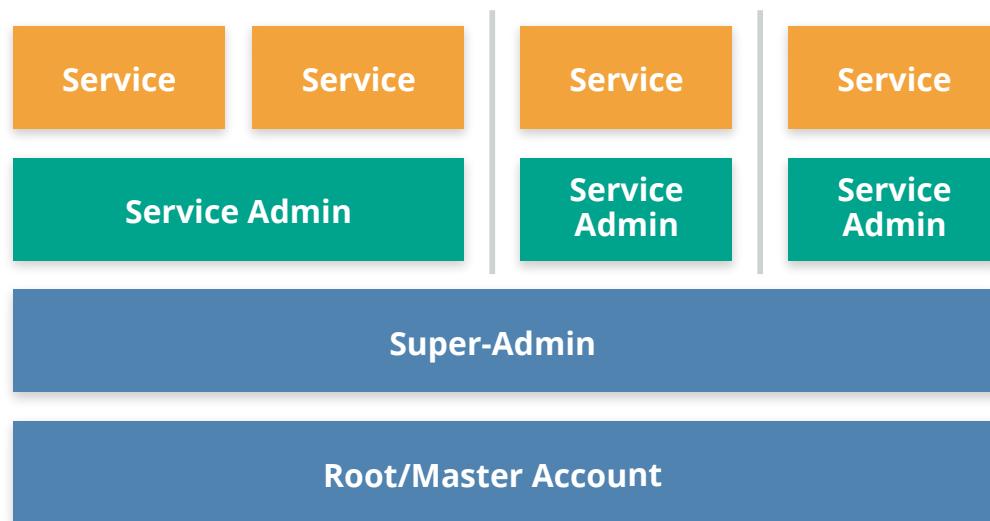
Identity and Access Management (IAM) includes identification, authentication, and authorizations (including access management). This is how you determine who can do what within your cloud platform or provider.

The specific options, configurations, and even concepts vary heavily between cloud providers and platforms. Each has their own implementation and may not even use the same definitions for things like “groups” and “roles.”

No matter the platform or provider there is always an account owner with super-admin privileges to manage the entire configuration. This should be enterprise-owned (not personal), tightly locked down, and nearly never used.

Separate from the account-owner you can usually create super-admin accounts for individual admin use. Use these privileges sparingly; this should also be a smaller group since compromise or abuse of one of these accounts could allow someone to change or access essentially everything and anything.

Your platform or provider may support lower-level administrative accounts that can only manage parts of the service. We sometimes call these “service administrators” or “day to day administrators”. These accounts don’t necessarily expose the entire deployment if they are abused or compromised and thus are better for common daily usage. They also help compartmentalize individual sessions, so it isn’t unusual to allow a single human administrator access to multiple service administrator accounts (or roles) so they can log in with just the privileges they need for that particular action instead of having to expose a much wider range of entitlements.



*Examples of baseline cloud management plane user accounts including super-administrators and service administrators.*

Both providers and consumers should consistently only allow the least privilege required for users, applications, and other management plane usage.

All privileged user accounts should use multi-factor authentication (MFA). If possible, *all* cloud accounts (even individual user accounts) should use MFA. It’s one of the single most effective security controls to defend against a wide range of attacks. This is also true regardless of the service model: MFA is just as important for SaaS as it is for IaaS.

(See the IAM domain for more information on IAM and the role of federation and strong authentication, much of which applies to the cloud management plane.)



### 6.1.1.3 Management Plane Security When Building/Providing a Cloud Service

When you are responsible for building and maintaining the management plane itself, such as in a private cloud deployment, that increases your responsibilities. When you consume the cloud you only configure the parts of the management plane that the provider exposes to you, but when you are the cloud provider you obviously are responsible for everything.

Delving into implementation specifics is beyond the scope of this Guidance, but at a high level there are five major facets to building and managing a secure management plane:

- *Perimeter security*: Protecting from attacks against the management plane's components itself, such as the web and API servers. It includes both lower-level network defenses as well as higher-level defenses against application attacks.
- *Customer authentication*: Providing secure mechanisms for customers to authenticate to the management plane. This should use existing standards (like OAuth or HTTP request signing) that are cryptographically valid and well documented. Customer authentication should support MFA as an option or requirement.
- *Internal authentication and credential passing*: The mechanisms your own employees use to connect with the non-customer-facing portions of the management plane. It also includes any translation between the customer's authentication and any internal API requests. Cloud providers should always mandate MFA for cloud management authentication.
- *Authorization and entitlements*: The entitlements available to customers and the entitlements for internal administrators. Granular entitlements better enable customers to securely manage their own users and administrators. Internally, granular entitlements reduce the impact of administrators' accounts being compromised or employee abuse.
- *Logging, monitoring, and alerting*: Robust logging and monitoring of administrative is essential for effective security and compliance. This applies both to what the customer does in their account, and to what employees do in their day-to-day management of the service. Alerting of unusual events is an important security control to ensure that monitoring is actionable, and not merely something you look at after the fact. Cloud customers should ideally be able to access logs of their own activity in the platform via API or other mechanism in order to integrate with their own security logging systems.

### 6.1.2 Business Continuity and Disaster Recovery

Like security and compliance, BC/DR is a shared responsibility. There are aspects that the cloud provider has to manage, but the cloud customer is also ultimately responsible for how they use and manage the cloud service. This is especially true when planning for outages of the cloud provider (or parts of the cloud provider's service).

Also similar to security, customers have more control and responsibility in IaaS, less in SaaS, with PaaS in the middle.

BC/DR must take a risk-based approach. Many BC options may be cost prohibitive in the cloud, but may also not be necessary. This is no different than in traditional data centers, but it isn't unusual



to want to over-compensate when losing physical control. For example, the odds of a major IaaS provider going out of business or changing their entire business model are low, but this isn't all that uncommon for a smaller venture-backed SaaS provider.

- Ask the provider for outage statistics over time since this can help inform your risk decisions.
- Remember that capabilities vary between providers and should be included in the vendor selection process.

#### 6.1.2.1 Business Continuity Within the Cloud Provider

When you deploy assets into the cloud you can't assume the cloud will always be there, or always work the way you expect. Outages and issues are no more or less common than with any other technology, although the cloud can be overall more resilient when the provider includes mechanisms to better enable building resilient applications.

This is a key point we need to spend a little more time on: As we've mentioned in a few places the very nature of virtualizing resources into pools typically creates less resiliency for any single asset, like a virtual machine. On the other hand, abstracting resources and managing everything through software opens up flexibility to more easily enable resiliency features like durable storage and cross-geographic load balancing.

There is a huge range of options here, and not all providers or platforms are created equal, but you shouldn't assume that "the cloud" as a general term is more or less resilient than traditional infrastructure. Sometimes it's better, sometimes it's worse, and knowing the difference all comes down to your risk assessment and how you use the cloud service.

This is why it is typically best to re-architect deployments when you migrate them to the cloud. Resiliency itself, and the fundamental mechanisms for ensuring resiliency, change. Direct "lift and shift" migrations are less likely to account for failures, nor will they take advantage of potential improvements from leveraging platform or service specific capabilities.

The focus is on understanding and leveraging the platform's BC/DR features. Once you make the decision to deploy in the cloud you then want to optimize your use of included BC/DR features before adding on any additional capabilities through third-party tools.

BC/DR must account for the entire logical stack:

- *Metastructure*: Since cloud configurations are controlled by software, these configurations should be backed up in a restorable format. This isn't always possible, and is pretty rare in SaaS, but there are tools to implement this in many IaaS platforms (including third-party options) using *Software-Defined Infrastructure*.
- *Software-Defined Infrastructure* allows you to create an infrastructure template to configure all or some aspects of a cloud deployment. These templates are then translated natively by the cloud platform or into API calls that orchestrate the configuration.



This should include controls such as IAM and logging, not merely architecture, network design, or service configurations.

- *Infrastructure*: As mentioned, any provider will offer features to support higher availability than can comparably be achieved in a traditional data center for the same cost. But these only work if you adjust your architecture. “Lifting and shifting” applications to the cloud without architectural adjustments or redesign will often result in lower availability.

Be sure and understand the cost model for these features, especially for implementing them across the provider’s physical locations/regions, where the cost can be high. Some assets and data must be converted to work across cloud locations/regions, for example, custom machine images used to launch servers. These assets must be included in plans.

- *Infostructure*: Data synchronization is often one of the more difficult issues to manage across locations, even if the actual storage costs are manageable. This is due to the size of data sets (vs. an infrastructure configuration) and keeping data in sync across locations and services, something that’s often difficult even in a single storage location/system.
- *Applistructure*: Applistructure includes all of the above, but also the application assets like code, message queues, etc. When a cloud user builds their own cloud applications they’re usually built on top of IaaS and/or PaaS, so resiliency and recovery are inherently tied to those layers. But Applistructure includes the full range of everything in an application.

Understand PaaS limitations and lock-ins, and plan for the outage of a PaaS component. Platform services include a range of functions we used to manually implement in applications, everything from authentication systems to message queues and notifications. It isn’t unusual for modern applications to even integrate these kinds of services from multiple different cloud providers, creating an intricate web.

Discussing availability of the component/service with your providers is reasonable. For example, the database service from your infrastructure provider may not share the same performance and availability as their virtual machine hosting.

When real-time switching isn’t possible, design your application to gracefully fail in case of a service outage. There are many automation techniques to support this. For example, if your queue service goes down, that should trigger halting the front end so messages aren’t lost.

Downtime is always an option. You don’t always need perfect availability, but if you do plan to accept an outage you should at least ensure you fail gracefully, with emergency downtime notification pages and responses. This may be possible using static stand-by via DNS redirection.

“Chaos Engineering” is often used to help build resilient cloud deployments. Since everything cloud is API-based, Chaos Engineering uses tools to selectively degrade portions of the cloud to continuously test business continuity.

This is often done in production, not just test environment, and forces engineers to assume



failure instead of viewing it as only a possible event. By designing systems for failure you can better absorb individual component failures.

#### 6.1.2.2 Business Continuity for Loss of the Cloud Provider

It is always possible that an entire cloud provider or at least a major portion of its infrastructure (such as one specific geography) can go down. Planning for cloud provider outages is difficult, due to the natural lock-in of leveraging a provider's capabilities. Sometimes you can migrate to a different portion of their service, but in other cases an internal migration simply isn't an option, or you may be totally locked in.

Depending on the history of your provider, and their internal availability capabilities, accepting this risk is often a legitimate option.

Downtime may be another option, but it depends on your recovery time objectives (RTO). However, some sort of static stand-by should be available via DNS redirection. Graceful failure should also include failure responses to API calls, if you offer APIs.

Be wary of selecting a secondary provider or service if said service may also be located or reliant on the same provider. It doesn't do you any good to use a backup storage provider if said provider happens to be based on the same infrastructure provider.

Moving data between providers can be difficult, but might be easy compared to moving metastructure, security controls, logging, and so on, which may be incompatible between platforms.

SaaS may often be the biggest provider outage concern, due to total reliance on the provider. Scheduled data extraction and archiving may be your only BC option outside of accepting downtime. Extracting and archiving to another cloud service, especially IaaS/PaaS, may be a better option than moving it to local/on-premises storage. Again, take a risk-based approach that includes the unique history of your provider.

Even if you have your data, you must have an alternate application that you know you can migrate it into. If you can't use the data, you don't have a viable recovery strategy.

Test, test, and test. This may often be easier than in a traditional data center because you aren't constrained by physical resources, and only pay for use of certain assets during the life of the test.

#### 6.1.2.3 Business Continuity For Private Cloud and Providers

This is completely on the provider's shoulders, and BC/DR includes everything down to the physical facilities. RTOs and RPOs will be stringent, since if the cloud goes down, everything goes down.

If you are providing services to others, be aware of contractual requirements, including data residency, when building your BC plans. For example, failing over to a different geography in a different legal jurisdiction may violate contracts or local laws.



## 6.2 Recommendations

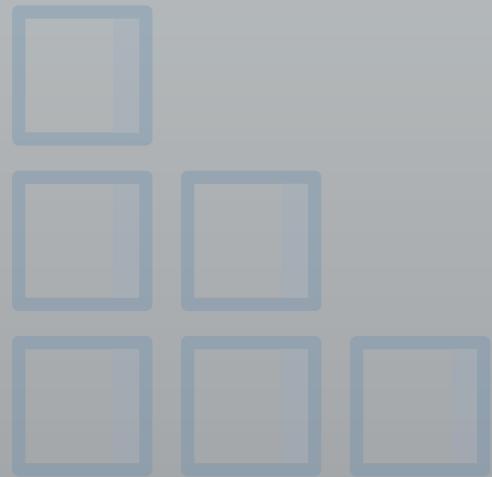
---

- Management plane (metastructure) security
  - Ensure there is strong perimeter security for API gateways and web consoles.
  - Use strong authentication and MFA.
  - Maintain tight control of primary account holder/root account credentials and consider dual-authority to access them.
    - Establishing multiple accounts with your provider will help with account granularity and to limit blast radius (with IaaS and PaaS).
  - Use separate super administrator and day-to-day administrator accounts instead of root/primary account holder credentials.
  - Consistently implement least privilege accounts for metastructure access.
    - This is why you separate development and test accounts with your cloud provider.
  - Enforce use of MFA whenever available.
- Business continuity
  - Architecture for failure.
  - Take a risk-based approach to everything. Even when you assume the worst, it doesn't mean you can afford or need to keep full availability if the worst happens.
  - Design for high availability within your cloud provider. In IaaS and PaaS this is often easier and more cost effective than the equivalent in traditional infrastructure.
    - Take advantage of provider-specific features.
    - Understand provider history, capabilities, and limitations.
    - Cross-location should always be considered, but beware of costs depending on availability requirements.
      - Also ensure things like images and asset IDs are converted to work in the different locations.
    - Business Continuity for metastructure is as important as that for assets.
  - Prepare for graceful failure in case of a cloud provider outage.
    - This can include plans for interoperability and portability with other cloud providers or a different region with your current provider.
  - For super-high-availability applications, start with cross-location BC before attempting cross-provider BC.
  - Cloud providers, including private cloud, must provide the highest levels of availability and mechanisms for customers/users to manage aspects of their own availability.



# DOMAIN 7

# Infrastructure Security



## 7.0 Introduction

Infrastructure security is the foundation for operating securely in the cloud. “Infrastructure” is the glue of computers and networks that we build everything on top of. For the purposes of this Guidance we start with compute and networking security, which also encompass workload and hybrid cloud. Although storage security is also core to infrastructure, it is covered in full depth in Domain 11: Data Security and Encryption. This domain also includes the fundamentals for private cloud computing. It does not include all the components of traditional data center security that are already well covered by existing standards and guidance.

Infrastructure security encompasses the lowest layers of security, from physical facilities through the consumer’s configuration and implementation of infrastructure components. These are the fundamental components that everything else in the cloud is built from, including compute (workload), networking, and storage security.

For purposes of the CSA Guidance we are focusing on cloud-specific aspects of infrastructure security. There are already incredibly robust bodies of knowledge and industry standards for data center security that cloud providers and private cloud deployments should reference. Consider this Guidance a layer on top of those extensive and widely available materials. Specifically, this Domain discusses two aspects: cloud considerations for the underlying infrastructure, and security for virtual networks and workloads.

## 7.1 Overview

In cloud computing there are two macro layers to infrastructure:

- The fundamental resources pooled together to create a cloud. This is the raw, physical and logical compute (processors, memory, etc.), networks, and storage used to build the cloud’s resource pools. For example, this includes the security of the networking hardware and software used to create the network resource pool.

- The virtual/abstracted infrastructure managed by a cloud user. That's the compute, network, and storage assets that they use from the resource pools. For example, the security of the virtual network, as defined and managed by the cloud user.

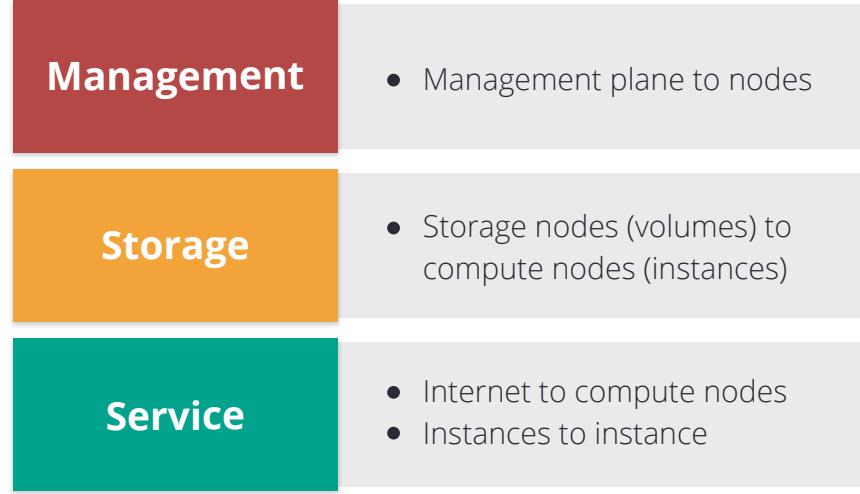
The information and advice in this domain primarily focuses on the second macro layer, infrastructure security for the cloud user. Infrastructure security that's more fundamental for cloud providers, including those who manage private clouds, is well aligned with existing security standards for data centers.

## 7.2 Cloud Network Virtualization

All clouds utilize some form of virtual networking to abstract the physical network and create a network resource pool. Typically the cloud user provisions desired networking resources from this pool, which can then be configured within the limits of the virtualization technique used. For example, some cloud platforms only support allocation of IP addresses within particular subnets, while others allow the cloud user the capability to provision entire Class B virtual networks and completely define the subnet architecture.

If you are a cloud provider (including managing a private cloud), physical segregation of networks composing your cloud is important for both operational and security reasons. We most commonly see at least three different networks which are isolated onto dedicated hardware since there is no functional or traffic overlap:

- The service network for communications between virtual machines and the Internet. This builds the network resource pool for the cloud users.
- The storage network to connect virtual storage to virtual machines.
- A management network for management and API traffic.



*Common networks underlying IaaS.*

This isn't the only way to build out a private cloud network architecture, but it is a common baseline, especially for private clouds that don't deal with the massive scale of public cloud providers but still need to balance performance and security.

There are two major categories of network virtualization commonly seen in cloud computing today:

- *Virtual Local Area Networks (VLANs)*: VLANs leverage existing network technology implemented in most network hardware. VLANs are extremely common in enterprise networks, even without



cloud computing. They are designed for use in single-tenant networks (enterprise data centers) to separate different business units, functions, etc. (like guest networks). VLANs are not designed for cloud-scale virtualization or security and shouldn't be considered, on their own, an effective security control for isolating networks. They are also never a substitute for physical network segregation.

- *Software Defined Networking (SDN)*: A more complete abstraction layer on top of networking hardware, SDNs decouple the network control plane from the data plane (you can [read more on SDN principles at this Wikipedia entry](#)). This allows us to abstract networking from the traditional limitations of a LAN.

There are multiple implementations, including standards-based and proprietary options. Depending on the implementation, SDN can offer much higher flexibility and isolation. For example, multiple segregated overlapping IP ranges for a virtual network on top of the same physical network. Implemented properly, and unlike standard VLANs, SDNs provide effective security isolation boundaries. SDNs also typically offer software definition of arbitrary IP ranges, allowing customers to better extend their existing networks into the cloud. If the customer needs the 10.0.0.0/16 CIDR (Classless Inter-Domain Routing) range, an SDN can support it, regardless of the underlying network addressing. It can typically even support multiple customers using the same internal networking IP address blocks.

On the surface, an SDN may look like a regular network to a cloud user, but being a more complete abstraction will function very differently beneath the surface. The underlying technologies and the management of the SDN will look nothing like what the cloud user accesses, and will have quite a bit more complexity. For example, an SDN may use packet encapsulation so that virtual machines and other "standard" assets don't need any changes to their underlying network stack. The virtualization stack takes packets from standard operating systems (OS) connecting through a virtual network interface, and then encapsulates the packets to move them around the actual network. The virtual machine doesn't need to have any knowledge of the SDN beyond a compatible virtual network interface, which is provided by the hypervisor.

## 7.3 How Security Changes With Cloud Networking

The lack of direct management of the underlying physical network changes common network practices for the cloud user and provider. The most commonly used network security patterns rely on control of the physical communication paths and insertion of security appliances. This isn't possible for cloud customers, since they only operate at a virtual level.

Traditional Network Intrusion Detection Systems, where communications between hosts are mirrored and inspected by the virtual or physical Intrusion Detection Systems will not be supported in cloud environments; customer security tools need to rely on an in-line virtual appliance, or a software agent installed in instances. This creates either a chokepoint or increases processor overhead, so be sure you really need that level of monitoring before implementing. Some cloud providers may offer some level of built-in network monitoring (and you have more options with private cloud platforms) but this isn't typically to the same degree as when sniffing a physical network.



### 7.3.1 Challenges of Virtual Appliances

Since physical appliances can't be inserted (except by the cloud provider) they must be replaced by virtual appliances if still needed, and if the cloud network supports the necessary routing. This brings the same concerns as inserting virtual appliances for network monitoring:

- Virtual appliances thus become bottlenecks, since they cannot fail open, and must intercept all traffic.
- Virtual appliances may take significant resources and increase costs to meet network performance requirements.
- When used, virtual appliances should support auto-scaling to match the elasticity of the resources they protect. Depending on the product, this could cause issues if the vendor does not support elastic licensing compatible with auto-scaling.
- Virtual appliances should also be aware of operating in the cloud, as well as the ability of instances to move between different geographic and availability zones. The *velocity* of change in cloud networks is higher than that of physical networks and tools need to be designed to handle this important difference.
- Cloud application components tend to be more distributed to improve resiliency and, due to auto-scaling, virtual servers may have shorter lives and be more prolific. This changes how security policies need to be designed.
  - This induces that very high rate of change that security tools must be able to manage (e.g., servers with a lifespan of less than an hour).
  - IP addresses will change far more quickly than on a traditional network, which security tools must account for. Ideally they should identify assets on the network by a unique ID, not an IP address or network name.
  - Assets are less likely to exist at static IP addresses. Different assets may share the same IP address within a short period of time. Alerts and the Incident Response lifecycle may have to be modified to ensure that the alert is actionable in such a dynamic environment. Assets within a single application tier will often be located on multiple subnets for resiliency, further complicating IP-based security policies. Due to auto-scaling, assets may also be ephemeral, existing for hours or even minutes. On the upside, cloud architectures skew towards fewer services per server, which improves your ability to define restrictive firewall rules. Instead of a stack of services on a single virtual machine — as on physical servers where you need to maximize the capital investment in the hardware — it is common to run a much smaller set of services, or even a single service, on a virtual machine.

### 7.3.2 SDN Security Benefits

On the positive side, software-defined networks enable new types of security controls, often making it an overall gain for network security:

- Isolation is easier. It becomes possible to build out as many isolated networks as you need without constraints of physical hardware. For example, if you run multiple networks with the same CIDR address blocks, there is no logical way they can directly communicate, due



to addressing conflicts. This is an excellent way to segregate applications and services of different security contexts. We discuss this microsegregation in more detail below.

- SDN firewalls (e.g., security groups) can apply to assets based on more flexible criteria than hardware-based firewalls, since they aren't limited based on physical topology. (Note that this is true of many types of software firewalls, but is distinct from hardware firewalls). SDN firewalls are typically policy sets that define ingress and egress rules that can apply to single assets or groups of assets, regardless of network location (within a given virtual network). For example, you can create a set of firewall rules that apply to any asset with a particular tag. Keep in mind this gets slightly difficult to discuss, since different platforms use different terminology and have different capabilities to support this kind of capability, so we are trying to keep things at a conceptual level.
  - Combined with the cloud platform's orchestration layer, this enables very dynamic and granular combinations and policies with less management overhead than the equivalent using a traditional hardware or host-based approach. For example, if virtual machines in an auto-scale group are automatically deployed in multiple subnets and load balanced across them, then you can create a firewall ruleset that applies to these instances, regardless of their subnet or IP address. It is a key enabling feature of secure cloud networks that use architectures quite differently from traditional computing.
  - Default deny is often the starting point, and you are required to open connections from there, which is the opposite of most physical networks.
    - Think of it as the granularity of a host firewall with the better manageability of a network appliance. Host firewalls have two issues: They are difficult to manage at scale, and if the system they are on is compromised, they are easy to alter and disable. On the other hand, it is cost-prohibitive to route all internal traffic, even between peers on a subnet, through a network firewall. Software firewalls, such as security groups, are managed outside a system yet apply to each system, without additional hardware costs or complex provisioning needed. Thus, it is trivial to do things like isolate every single virtual machine on the same virtual subnet.
    - As briefly mentioned above, firewall rules can be based on other criteria, such as tags. Note, that while the potential is there, the actual capabilities depend on the platform. Just because a cloud network is SDN-based doesn't mean it actually conveys any security benefits.
    - Many network attacks are eliminated by default (depending on your platforms), such as ARP spoofing and other lower level exploits, beyond merely eliminating sniffing. This is due to the inherent nature of the SDN and application of more software-based rules and analysis in moving packets.
    - It is possible to encrypt packets as they are encapsulated.
    - As with security groups, other routing and network design can be dynamic and tied to the cloud's orchestration layer, such as bridging virtual networks or connecting to internal PaaS services.
    - Additional security functions can potentially be added natively.

### 7.3.3 Microsegmentation and the Software Defined Perimeter

*Microsegmentation* (also sometimes referred to as *hypersegregation*) leverages virtual network topologies to run more, smaller, and more isolated networks without incurring additional hardware costs that historically make such models prohibitive. Since the entire networks are defined in software without many of the traditional addressing issues, it is far more feasible to run these multiple, software-defined environments.

A common, practical example leveraging this capability is running most, if not all, applications on their own virtual network and only connecting those networks as needed. This dramatically reduces the *blast radius* if an attacker compromises an individual system. The attacker can no longer leverage this foothold to expand across the entire data center.

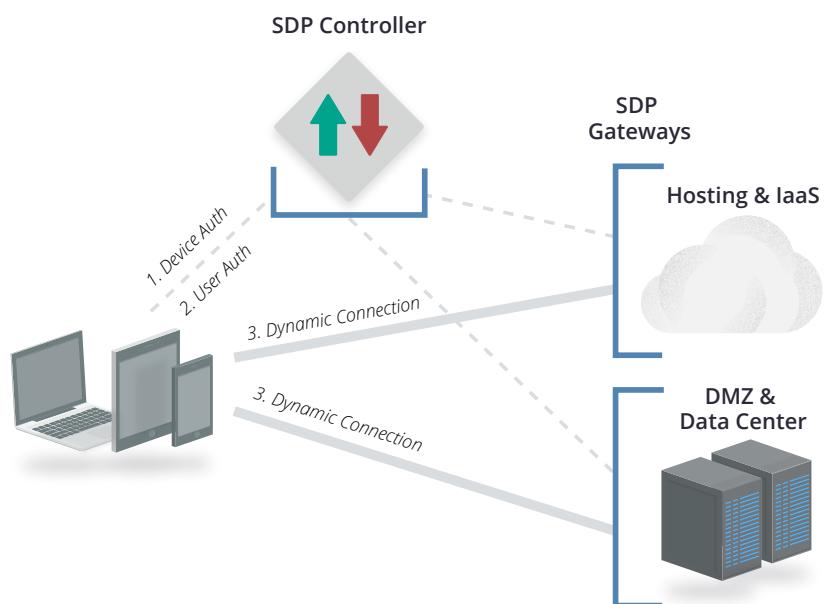
Although there are no increases in capital expenses since cloud microsegmentation is based on software configurations, it *can* increase operational expenses in managing multiple overlapping networks and connectivity.

The CSA **Software Defined Perimeter Working Group** has developed a model and specification that combines device and user authentication to dynamically provision network access to resources and enhance security. SDP includes three components:

- An SDP client on the connecting asset (e.g. a laptop).
- The SDP controller for authenticating and authorizing SDP clients and configuring the connections to SDP gateways.
- The SDP gateway for terminating SDP client network traffic and enforcing policies in communication with the SDP controller.

Network security decisions can thus be made on a wider range of criteria than just IP packets. Especially combined with SDNs this potentially offers greater flexibility and security for evolving network topologies.

More information on SDP is available from the CSA at [https://cloudsecurityalliance.org/group/software-defined-perimeter/#\\_overview](https://cloudsecurityalliance.org/group/software-defined-perimeter/#_overview)



*Common networks underlying IaaS.*

### **7.3.4 Additional Considerations for Cloud Providers or Private Clouds**

Providers must maintain the core security of the physical/traditional networks that the platform is built on. A security failure at the root network will likely compromise the security of all customers. And this security must be managed for arbitrary communications and multiple tenants, some of which must be considered adversarial.

It is absolutely critical to maintain segregation and isolation for the multitenant environment. There will thus be additional overhead to properly enable, configure, and maintain the SDN security controls. While an SDN is more likely to provide needed isolation once it is up and running, it is important to take the extra time to get everything set up properly in order to handle potentially hostile tenants. We aren't saying your users are necessarily hostile, but it is safe to assume that, at some point, something on the network will be compromised and used to further an attack.

Providers must also expose security controls to the cloud users so they can properly configure and manage their network security.

Finally, providers are responsible for implementing perimeter security that protects the environment, but minimizes impact on customer workloads, for example, Distributed Denial of Service Protection (DDoS) and baseline IPS to filter out hostile traffic before it affects the cloud's consumers. Another consideration is to ensure that any potentially sensitive information is scrubbed when a virtual instance is released back to the hypervisor, to ensure the information is not able to be read by another customer when the drive space is provisioned.

### **7.3.5 Hybrid Cloud Considerations**

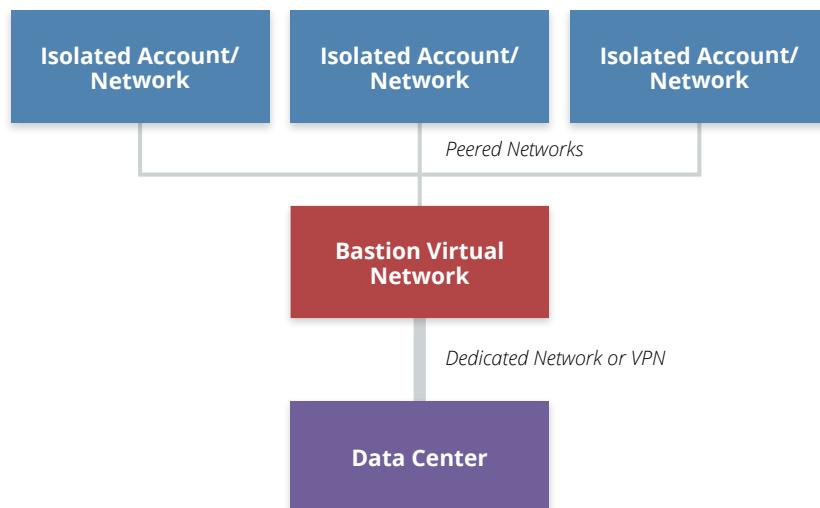
As mentioned in Domain 1, hybrid clouds connect an enterprise private cloud or data center to a public cloud provider, typically using either a dedicated Wide Area Network (WAN) link or VPN. Ideally the hybrid cloud will support arbitrary network addressing to help seamlessly extend the cloud user's network. If the cloud uses the same network address range as your on-premises assets, it is effectively unusable.

The hybrid connection may reduce the security of the cloud network if the private network isn't at an equivalent security level. If you run a flat network in your data center, with minimal segregation from your employees' systems, someone could compromise an employee's laptop and then use that to scan your entire cloud deployment over the hybrid connection. A hybrid connection shouldn't effectively flatten the security of both networks. Separation should be enforced via routing, access controls, and even firewalls or additional network security tools between the two networks.

For management and security reasons it is typically preferable to minimize hybrid connections. Connecting multiple disparate networks is complex, especially when one of those networks is software-defined and the other limited by hardware. Hybrid connections are often still necessary, but don't assume they are needed. They may increase routing complexity, can reduce the ability to run multiple cloud networks with overlapping IP ranges, and complicate security on both sides, due to the need to harmonize security controls.

One emerging architecture for hybrid cloud connectivity is “bastion” or “transit” virtual networks:

- This scenario allows you to connect multiple, different cloud networks to a data center using a single hybrid connection. The cloud user builds a dedicated virtual network for the hybrid connection and then peers any other networks through the designated bastion network.
- Second-level networks connect to the data center through the bastion network, but since they aren't peered to each other they can't talk to each other and are effectively segregated. Also, you can deploy different security tools, firewall rulesets, and Access Control Lists in the bastion network to further protect traffic in and out of the hybrid connection.



*“Bastion” or “Transit” networks for more-flexible hybrid cloud architectures.*

## 7.4 Cloud Compute and Workload Security

A workload is a unit of processing, which can be in a virtual machine, a container, or other abstraction. Workloads always run somewhere on a processor and consume memory. Workloads include a very diverse range of processing tasks, which range from traditional applications running in a virtual machine on a standard operating system, to GPU- or FPGA-based specialized tasks. Nearly every one of these options is supported in some form in cloud computing.

It's important to remember that every cloud workload runs on a hardware stack, and the integrity of this hardware is absolutely critical for the cloud provider to maintain. Different hardware stacks also support different execution isolation and chain of trust options. This can include hardware-based supervision and monitoring processes that run outside the main processors, secure execution environments, encryption and key management enclaves, and more. The range and rapidly changing nature of these options exceeds our ability to provide prescriptive guidance at this time, but in a general sense there are potentially very large gains in security by selecting and properly leveraging hardware with these advanced capabilities.

There are multiple compute abstraction types, each with differing degrees of segregation and isolation:

- *Virtual machines*: Virtual machines are the most-well known form of compute abstraction, and are offered by all IaaS providers. They are commonly called instances in cloud computing since they are created (or cloned) off a base image. The Virtual Machine Manager (hypervisor) abstracts an operating system from the underlying hardware. Modern hypervisors can tie into underlying hardware capabilities now commonly available on standard servers (and workstations) to reinforce isolation while supporting high-performance operations.

Virtual machines are potentially open to certain memory attacks, but this is increasingly difficult due to ongoing hardware and software enhancements to reinforce isolation. VMs on modern hypervisors are generally an effective security control, and advances in hardware isolation for VMs and secure execution environments continue to improve these capabilities.

- *Containers*: Containers are code execution environments that run within an operating system (for now), sharing and leveraging resources of that operating system. While a VM is a full abstraction of an operating system, a container is a constrained place to run segregated processes while still utilizing the kernel and other capabilities of the base OS. Multiple containers can run on the same virtual machine or be implemented without the use of VMs at all and run directly on hardware. The container provides code running inside a restricted environment with only access to the processes and capabilities defined in the container configuration. This allows containers to launch incredibly rapidly, since they don't need to boot an operating system or launch many (sometimes any) new services; the container only needs access to already-running services in the host OS and some can launch in milliseconds.

Containers are newer, with differing isolation capabilities that are very platform-dependent. They are also evolving quickly with different management systems, underlying operating systems, and container technologies. We cover containers in more depth in Domain 8.

- *Platform-based workloads*: This is a more complex category that covers workloads running on a shared platform that aren't virtual machines or containers, such as logic/procedures running on a shared database platform. Imagine a stored procedure running inside a multitenant database, or a machine-learning job running on a machine-learning Platform as a Service. Isolation and security are totally the responsibility of the platform provider, although the provider may expose certain security options and controls.
- *Serverless computing*: Serverless is a broad category that refers to any situation where the cloud user doesn't manage any of the underlying hardware or virtual machines, and just accesses exposed functions. For example, there are serverless platforms for directly executing application code. Under the hood, these still utilize capabilities such as containers, virtual machines, or specialized hardware platforms. From a security perspective, serverless is merely a combined term that covers containers and platform-based workloads, where the cloud provider manages all the underlying layers, including foundational security functions and controls.

### 7.4.1 How Cloud Changes Workload Security

Any given processor and memory will nearly always be running multiple workloads, often from different tenants. Multiple tenants will likely share the same physical compute node, and there is a range of segregation capabilities on different hardware stacks. The burden to maintain workload isolation is on the cloud provider and should be one of their top priorities.

In some environments dedicated/private tenancy is possible, but typically at a higher cost. With this model only designated workloads run on a designated physical server. Costs increase in public cloud as a consumer since you are taking hardware out of the general resource pool, but also in private cloud, due to less efficient use of internal resources.

Cloud users rarely get to control where a workload physically runs, regardless of deployment model, although some platforms do support designating particular hardware pools or general locations to support availability, compliance, and other requirements.

### 7.4.2 Immutable Workloads Enable Security

Auto-scaling and containers, by nature, work best when you run instances launched dynamically based on an image; those instances can be shut down when no longer needed for capacity without breaking an application stack. This is core to the elasticity of compute in the cloud. Thus, you no longer patch or make other changes to a running workload, since that wouldn't change the image, and, thus, new instances would be out of sync with whatever manual changes you make on whatever is running. We call these virtual machines *immutable*.

To reconfigure or change an immutable instance you update the underlying image, and then rotate the new instances by shutting down the old ones and running the new ones in their place.

There are degrees of immutable. The pure definition is fully replacing running instances with a new image. However, some organizations only push new images to update the operating system and use alternative deployment techniques to push code updates into running virtual machines. While technically not completely immutable, since the instance changes, these pushes still happen completely through automation and no one ever manually logs in to running systems to make local changes.

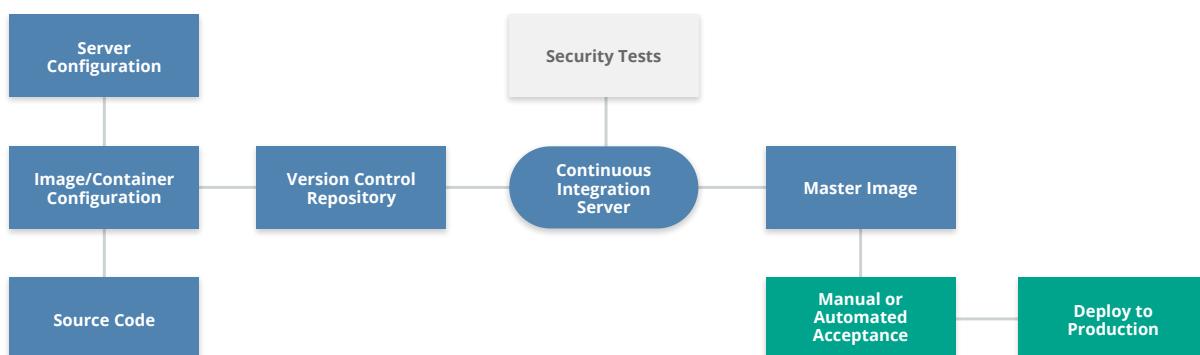
Immutable workloads enable significant security benefits:

- You no longer patch running systems or worry about dependencies, broken patch processes, etc. You replace them with a new gold master.
- You can, and should, disable remote logins to running workloads (if logins are even an option). This is an operational requirement to prevent changes that aren't consistent across the stack, which also has significant security benefits.
- It is much faster to roll out updated versions, since applications must be designed to handle individual nodes going down (remember, this is fundamental to any auto-scaling). You are less constrained by the complexity and fragility of patching a running system. Even if something breaks, you just replace it.

- It is easier to disable services and whitelist applications/processes since the instance should never change.
- Most security testing can be managed during image creation, reducing the need for vulnerability assessment on running workloads since their behavior should be completely known at the time of creation. This doesn't eliminate all security testing for production workloads, but it is a means of offloading large portions of testing.

Immutable does add some requirements:

- You need a consistent image creation process and the automation to support updating deployments. These new images must be produced on a regular basis to account for patch and malware signature updates.
- Security testing must be integrated into the image creation and deployment process, including source code tests and, if using virtual machines or standard containers, vulnerability assessments.
- Image configurations need mechanisms to disable logins and restrict services before deploying the images and using them for production virtual machines.
- You may want a process, for some workloads, to enable logins to workloads that aren't actively in the application stack for troubleshooting. This could be a workload pulled from the group but allowed to continue to run in isolation. Alternatively (and often preferred), send sufficiently detailed logs to an external collector so that there is never a need to log in.
- There will be increased complexity to manage the service catalog, since you might create dozens, or even hundreds, of images on any given day.



*A deployment pipeline for creating images for immutable virtual machines or containers.*



### 7.4.3 The Impact of Cloud on Standard Workload Security Controls

Some standard workload controls aren't as viable in cloud workloads (e.g. running antivirus inside some container types). Others aren't necessarily needed or need deep modification to maintain effectiveness in cloud computing:

- You may lose the ability to run software agents for non-VM based workloads, such as those running in "serverless" provider-managed containers.
- "Traditional" agents may impede performance more heavily in cloud. Lightweight agents with lower compute requirements allow better workload distribution and efficient use of resources. Agents not designed for cloud computing may assume underlying compute capacity that isn't aligned with how the cloud deployment is designed. The developers on a given project might assume they are running a fleet of lightweight, single-purpose virtual machines. A security agent not attuned to this environment could significantly increase processing overhead, requiring larger virtual machine types and increasing costs.
- Agents that operate in cloud environments also need to support dynamic cloud workloads and deployment patterns like auto-scaling. They can't rely (on the agent or in the management system) on static IP addressing. While some cloud assets run on static IP addresses, it is far more common for the cloud to dynamically assign IP addresses at run time to enable elasticity. Thus, the agent must have the ability to discover the management/control plane and use that to determine what kind of workload it is running on and where.
- The management plane of the agent must itself also operate at the speed of auto-scaling and support elasticity (e.g., be able to keep up with incredibly dynamic IP addressing, such as the same address used by multiple workloads within a single hour). Traditional tools aren't normally designed for this degree of velocity, creating the same issue as we discussed with network security and firewalls.
- Agents shouldn't increase attack surface due to communications/networking or other requirements that increase the attack surface. While this is always true, there is a greater likelihood of an agent becoming a security risk in cloud for a few reasons:
  - We have a greater ability to run immutable systems, and an agent, like any piece of software, opens up additional attack surface, especially if it ingests configuration changes and signatures that could be used as an attack vector.
  - In cloud we also tend to run fewer different services with a smaller set of networking ports on any given virtual machine (or container), as compared to a physical server. Some agents require opening up additional firewall ports, which increases the network attack surface.
  - This doesn't mean agents always create new security risks, but the benefits need to be balanced before simply assuming the security upside.
- File integrity monitoring can be an effective means of detecting unapproved changes to running immutable instances. Immutable workloads typically require fewer additional security tools, due to their hardened nature. They are locked down more than the usual servers and tend to run a smaller set of services. File integrity monitoring, which tends to be very lightweight, can be a good security control for immutable workloads since you should essentially have zero false positives by their unchanging nature.
- Long-running VMs that still run standard security controls may be isolated on the network, changing how they are managed. You might experience difficulty in connecting your



management tool to a virtual machine running in a private network subnet. While you can technically run the management tool in the same subnet, this could increase costs significantly and be more difficult to manage.

- Cloud workloads running in isolation are typically less resilient than on physical infrastructure, due to the abstraction. Providing disaster recovery for these is extremely important.

#### **7.4.4 Changes to Workload Security Monitoring and Logging**

Security logging/monitoring is more complex in cloud computing:

- IP addresses in logs won't necessarily reflect a particular workflow since multiple virtual machines may share the same IP address over a period of time, and some workloads like containers and serverless may not have a recognizable IP address at all. Thus, you need to collect some other unique identifiers in the logs to be assured you know what the log entries actually refer to. These unique identifiers need to account for ephemeral systems, which may only be active for a short period of time.
- Logs need to be offloaded and collected externally more quickly due to the higher velocity of change in cloud. You can easily lose logs in an auto-scale group if they aren't collected before the cloud controller shuts down an unneeded instance.
  - Logging architectures need to account for cloud storage and networking costs. For example, sending all logs from instances in a public cloud to on-premises Security Information and Event Management (SIEM) may be cost prohibitive, due to the additional internal storage and extra Internet networking fees.

#### **7.4.5 Changes to Vulnerability Assessment**

Vulnerability assessments in cloud computing need to account for both architectural and contractual limitations:

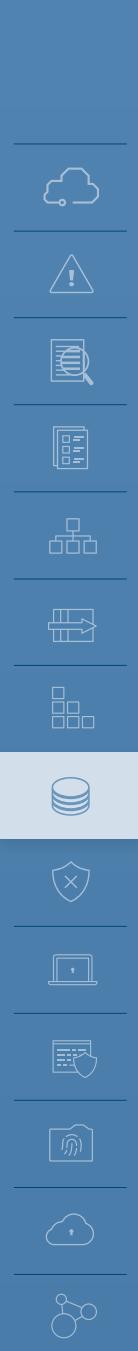
- The cloud owner (public or private) will typically require notification of assessments and place limits on the nature of assessments. This is because they may be unable to distinguish an assessment from a real attack without prior warning.
- Default deny networks further limit the potential effectiveness of an automated network assessment, just as any firewall would. You either need to open up holes to perform the assessment, use an agent on the instance to perform the assessment, or assess knowing that a lot of tests are blocked by the firewall rules.
- Assessments can be run during the image creation process for immutable workloads. Since these aren't in production, and the process is automated, they can run with fewer network restrictions, thus increasing the assessment surface.
- Penetration testing is less affected since it still uses the same scope as an attacker. We cover penetration testing in more detail in Domain 10.

#### **7.4.6 Cloud Storage Security**

Although part of infrastructure, we cover storage and data security in much more depth in Domain 11.

## 7.5 Recommendations

- Know the infrastructure security of your provider or platform.
  - In the shared security model, the provider (or whoever maintains the private cloud platform) has the burden of ensuring the underlying physical, abstraction, and orchestration layers of the cloud are secure.
  - Review compliance certifications and attestations.
    - Check industry-standard and industry-specific compliance certifications and attestations on a regular basis for having the assurance that your provider is following cloud infrastructure best-practices and regulations.
- Network
  - Prefer SDN when available.
  - Use SDN capabilities for multiple virtual networks and multiple cloud accounts/segments to increase network isolation.
    - Separate accounts and virtual networks dramatically limit blast radius compared to traditional data centers.
  - Implement default deny with cloud firewalls.
  - Apply cloud firewalls on a per-workload basis as opposed to a per-network basis.
  - Always restrict traffic between workloads in the same virtual subnet using a cloud firewall (security group) policy whenever possible.
  - Minimize dependency on virtual appliances that restrict elasticity or cause performance bottlenecks.
- Compute/workload
  - Leverage immutable workloads whenever possible.
    - Disable remote access.
    - Integrate security testing into image creation.
    - Alarm with file integrity monitoring.
    - Patch by updating images, not patching running instances.
    - Choose security agents that are cloud-aware and minimize performance impact, if needed.
  - Maintain security controls for long-running workloads, but use tools that are cloud aware.
  - Store logs external to workloads.
  - Understand and comply with cloud provider limitations on vulnerability assessments and penetration testing.



# DOMAIN 8

# Virtualization and Containers



## 8.0 Introduction

Virtualization isn't merely a tool for creating virtual machines—it's the core technology for enabling cloud computing. We use virtualization all throughout computing, from full operating virtual machines to virtual execution environments like the Java Virtual Machine, as well as in storage, networking, and beyond.

Cloud computing is fundamentally based on pooling resources and virtualization is the technology used to convert fixed infrastructure into these pooled resources. Virtualization provides the abstraction needed for resource pools, which are then managed using orchestration.

As mentioned, virtualization covers an extremely wide range of technologies; essentially any time we create an abstraction, we're using virtualization. For cloud computing we tend to focus on those specific aspects of virtualization used to create our resource pools, especially:

- Compute
- Network
- Storage
- Containers

The aforementioned aren't the only categories of virtualization, but they are the ones most relevant to cloud computing.

Understanding the impacts of virtualization on security is fundamental to properly architecting and implementing cloud security. Virtual assets provisioned from a resource pool may look just like the physical assets they replace, but that look and feel is really just a tool to help us better understand and manage what we see. It's also a useful way to leverage existing technologies, like operating systems, without having to completely rewrite them from scratch. Underneath, these virtual assets work completely differently from the resources they are abstracted from.

# 8.1 Overview

At its most basic, virtualization abstracts resources from their underlying physical assets. You can virtualize nearly anything in technology, from entire computers to networks to code. As mentioned in the introduction, cloud computing is fundamentally based on virtualization: It's how we abstract resources to create pools. Without virtualization, there is no cloud.

Many security processes are designed with the expectation of physical control over the underlying infrastructure. While this doesn't go away with cloud computing, virtualization adds two new layers for security controls:

- *Security of the virtualization technology itself*, e.g., securing a hypervisor.
- *Security controls for the virtual assets*. In many cases, this must be implemented differently than it would be in the corresponding physical equivalent. For example, as discussed in Domain 7, virtual firewalls are not the same as physical firewalls, and mere abstraction of a physical firewall into a virtual machine still may not meet deployment or security requirements.

Virtualization security in cloud computing still follows the shared responsibility model. The cloud provider will always be responsible for securing the physical infrastructure and the virtualization platform itself. Meanwhile, the cloud customer is responsible for properly implementing the available virtualized security controls and understanding the underlying risks, based on what is implemented and managed by the cloud provider. For example, deciding when to encrypt virtualized storage, properly configuring the virtual network and firewalls, or deciding when to use dedicated hosting vs. a shared host.

Since many of these controls touch upon other areas of cloud security, such as data security, we try to focus on the virtualization-specific concerns in this domain. The lines aren't always clear, however, and the bulk of cloud security controls are covered more deeply in the other domains of this Guidance. Domain 7: Infrastructure Security focuses extensively on virtual networks and workloads.

## 8.1.1 Major Virtualization Categories Relevant to Cloud Computing

### 8.1.1.1 Compute

Compute virtualization abstracts the running of code (including operating systems) from the underlying hardware. Instead of running directly on the hardware, the code runs on top of an abstraction layer that enables more flexible usage, such as running multiple operating systems on the same hardware (virtual machines). This is a simplification, and we recommend further research into virtual machine managers and hypervisors if you are interested in learning more.

Compute most commonly refers to virtual machines, but this is quickly changing, in large part due to ongoing technology evolution and adoption of containers.

Containers and certain kinds of serverless infrastructure also abstract compute. These are different abstractions to create code execution environments, but they don't abstract a full operating system



as a virtual machine does. (Containers are covered in more detail below.)

### ***Cloud Provider Responsibilities***

The primary security responsibilities of the cloud provider in compute virtualization are to enforce *isolation* and maintain a *secure virtualization infrastructure*.

- *Isolation* ensures that compute processes or memory in one virtual machine/container should not be visible to another. It is how we separate different tenants, even when they are running processes on the same physical hardware.
- The cloud provider is also responsible for securing the *underlying infrastructure and the virtualization technology* from external attack or internal misuse. This means using patched and up-to-date hypervisors that are properly configured and supported with processes to keep them up to date and secure over time. The inability to patch hypervisors across a cloud deployment could create a fundamentally insecure cloud when a new vulnerability in the technology is discovered.

Cloud providers should also support secure use of virtualization for cloud users. This means creating a secure chain of processes from the image (or other source) used to run the virtual machine all the way through a boot process with security and integrity. This ensures that tenants cannot launch machines based on images that they shouldn't have access to, such as those belonging to another tenant, and that a running virtual machine (or other process) is the one the customer expects to be running.

In addition, cloud providers should assure customers that volatile memory is safe from unapproved monitoring, since important data could be exposed if another tenant, a malicious employee, or even an attacker is able to access running memory.

### ***Cloud User Responsibilities***

Meanwhile, the primary responsibility of the cloud user is to properly implement the security of whatever it deploys within the virtualized environment. Since the onus of compute virtualization security is on the provider, the customer tends to have only a few security options relating directly to the virtualization of the workload. There is quite a bit more to securing workloads, and those are covered in Domain 7.

That said, there are still some virtualization-specific differences that the cloud user can address in their security implementation. Firstly, the cloud user should take advantage of the security controls for managing their virtual infrastructure, which will vary based on the cloud platform and often include:

- *Security settings, such as identity management, to the virtual resources.* This is not the identity management within the resource, such as the operating system login credentials, but the identity management of who is allowed to access the cloud management of the resource—for example, stopping or changing the configuration of a virtual machine. See Domain 6 for specifics on management plane security.

- *Monitoring and logging.* Domain 7 covers monitoring and logging of workloads, including how to handle system logs from virtual machines or containers, but the cloud platform will likely offer additional logging and monitoring at the virtualization level. This can include the status of a virtual machine, management events, performance, etc.
- *Image asset management.* Cloud compute deployments are based on master images—be it a virtual machine, container, or other code—that are then run in the cloud. This is often highly automated and results in a larger number of images to base assets on, compared to traditional computing master images. Managing these—including which meet security requirements, where they can be deployed, and who has access to them—is an important security responsibility.
- *Use of dedicated hosting,* if available, based on the security context of the resource. In some situations you can specify that your assets run on hardware dedicated only to you (at higher cost), even on a multitenant cloud. This may help meet compliance requirements or satisfy security needs in special cases where sharing hardware with another tenant is considered a risk.

Secondly, the cloud user is also responsible for security controls within the virtualized resource:

- This includes all the standard security for the workload, be it a virtual machine, container, or application code. These are well covered by standard security, best practices and the additional guidance in Domain 7.
- Of particular concern is ensuring deployment of only secure configurations (e.g., a patched, updated virtual machine image). Due to the automation of cloud computing it is easy to deploy older configurations that may not be patched or properly secured.

Other general compute security concerns include:

- Virtualized resources tend to be more ephemeral and change at a more rapid pace. Any corresponding security, such as monitoring, must keep up with the pace. Again, the specifics are covered in more depth in Domain 7.
- Host-level monitoring/logging may not be available, especially for serverless deployments. Alternative log methods may need to be implemented. For example, in a serverless deployment, you are unlikely to see system logs of the underlying platform and should offset by writing more robust application logging in to your code.

## **8.1.2 Network**

There are multiple kinds of virtual networks, from basic VLANs to full Software-Defined Networks. As a core of cloud infrastructure security these are covered both here and in Domain 7.

To review, most cloud computing today uses SDN for virtualizing networks. (VLANs are often not suitable for cloud deployments since they lack important isolation capabilities for multitenancy.)

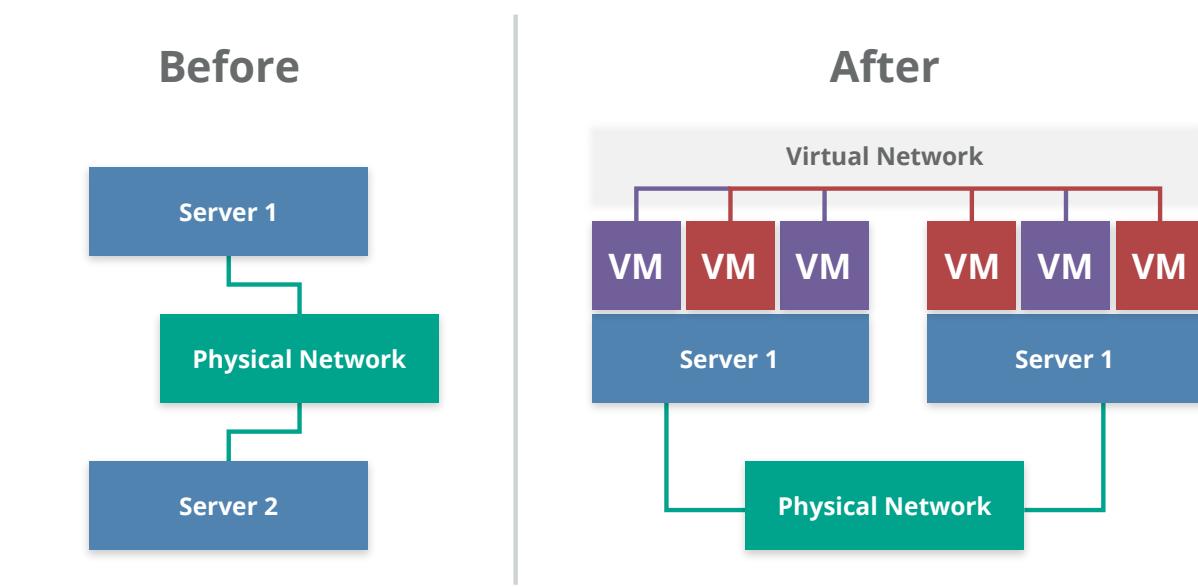
SDN abstracts the network management plane from the underlying physical infrastructure, removing many typical networking constraints. For example, you can overlay multiple virtual

networks, even ones that completely overlap their address ranges, over the same physical hardware, with all traffic properly segregated and isolated. SDNs are also defined using software settings and API calls, which supports orchestration and agility.

Virtual networks are quite different than physical networks. They run on physical networks, but abstraction allows for deep modification on networking behavior in ways that impact many security processes and technologies.

#### 8.1.2.1 Monitoring and Filtering

In particular, monitoring and filtering (including firewalls) change extensively due to the differences in how packets move around the virtual network. Resources may communicate on a physical server without traffic crossing the physical network. For example, if two virtual machines are located on the same physical machine there is no reason to route network traffic off the box and onto the network. Thus, they can communicate directly, and monitoring and filtering tools inline on the network (or attached to the routing/switching hardware) will never see the traffic.



*Virtual networks move packets in software and monitoring can't rely on sniffing the physical network connections.*

To compensate, you can route traffic to a virtual network monitoring or filtering tool on the same hardware (including a virtual machine version of a network security product). You can also bridge all network traffic back out to the network, or route it to a virtual appliance on the same virtual network. Each of these approaches has drawbacks since they create bottlenecks and less-efficient routing.

The cloud platform/provider may not support access for direct network monitoring. Public cloud providers rarely allow full packet network monitoring to customers, due to the complexity (and cost). Thus, you can't assume you will ever have access to raw packet data unless you collect it yourself in the host, or using a virtual appliance.

With public cloud in particular, some communications between cloud services will occur on the



provider's network; customer monitoring and filtering of that traffic isn't possible (and would create a security risk for the provider). For example, if you connect a serverless application to the cloud provider's object storage, database platform, message queue, or other PaaS product, this traffic would run natively on the provider's network, not necessarily within the customer-managed virtual network. As we move out of simple infrastructure virtualization, the concept of a customer-managed network begins to fade.

However, all modern cloud platforms offer built-in firewalls, which may offer advantages over corresponding physical firewalls. These are software firewalls that may operate within the SDN or the hypervisor. They typically offer fewer features than a modern, dedicated next-generation firewall, but these capabilities may not always be needed due to other inherent security provided by the cloud provider.

### 8.1.2.2 Management Infrastructure

Virtual networks for cloud computing always support remote management and, as such, securing the management plane/metastructure is critical. At times it is possible to create and destroy entire complex networks with a handful of API calls or a few clicks on a web console.

#### ***Cloud Provider Responsibilities***

The cloud provider is primarily responsible for building a secure network infrastructure and configuring it properly. The absolute top security priority is segregation and isolation of network traffic to prevent tenants from viewing another's traffic. This is the most foundational security control for any multitenant network.

The provider should disable packet sniffing or other metadata "leaks" that could expose data or configurations between tenants. Packet sniffing, even within a tenant's own virtual networks, should also be disabled to reduce the ability of an attacker to compromise a single node and use it to monitor the network, as is common on non-virtualized networks. Tagging or other SDN-level metadata should also not be exposed outside the management plane or a compromised host could be used to span into the SDN itself.

All virtual networks should enable built-in firewall capabilities for cloud users without the need for host firewalls or external products. The provider is also responsible for detecting and preventing attacks on the underlying physical network and virtualization platform. This includes perimeter security of the cloud itself.

#### ***Cloud User Responsibilities***

Cloud users are primarily responsible for properly configuring their deployment of the virtual network, especially any virtual firewalls.

Network architecture can play a larger role in virtual network security since we aren't constrained by physical connections and routing. Since virtual networks are software constructs, the use of multiple, separate virtual networks may offer extensive compartmentalization advantages not possible



on a traditional physical network. You can run every application stack in its own virtual network, which dramatically reduces the attack surface if a malicious actor gains a foothold. An equivalent architecture on a physical network is cost prohibitive.

*Immutable* networks can be defined on some cloud platforms using software templates, which can help enforce known-good configurations. The entire known-good state of the network can be defined in a template, instead of having to manually configure all the settings. Aside from the ability to create multiple networks with a secure baseline, these can also be used to detect, and in some cases revert, deviations from known-good states.

The cloud user is, again, responsible for proper rights management and configuration of exposed controls in the management plane. When virtual firewalls and/or monitoring don't meet security needs, the consumer may need to compensate with a virtual security appliance or host security agent. This falls under cloud infrastructure security and is covered in depth in Domain 7.

### **8.1.2.3 Cloud Overlay Networks**

Cloud overlay networks are a special kind of WAN virtualization technology for created networks that span multiple "base" networks. For example, an overlay network could span physical and cloud locations or multiple cloud networks, perhaps even on different providers. A full discussion is beyond the scope of this Guidance and the same core security recommendations apply.

## **8.1.3 Storage**

Storage virtualization is already common in most organizations—Storage Area Network (SAN) and Network-Attached Storage (NAS) are both common forms of storage virtualization—and storage security is discussed in more detail in Domain 11.

Most virtualized storage is durable and keeps multiple copies of data in different locations so that drive failures are less likely to result in data loss. Encrypting those drives reduces the concern that swapping out a drive, which is a very frequent activity, could result in data exposure.

However, this encryption doesn't protect data in any virtualized layers; it only protects the data at physical storage. Depending on the type of storage the cloud provider may also (or instead) encrypt it at the virtualization layer, but this may not protect customer data from exposure to the cloud provider. Thus, any additional protection should be provided using the advice in Domain 11.

## **8.1.4 Containers**

Containers are highly portable code execution environments. To simplify, a virtual machine is a complete operating system, all the way down to the kernel. A container, meanwhile, is a virtual execution environment that features an isolated user space, but uses a shared kernel. A full discussion is beyond the scope of this guidance and [you can read more about software containers at this Wikipedia entry](#).



Such containers can be built directly on top of physical servers or run on virtual machines. Current implementations rely on an existing kernel/operating system, which is why they can run inside a virtual machine even if nested virtualization is not supported by the hypervisor. (Software containers rely on a completely different technology for hypervisors.)

Software container systems always include three key components:

- The execution environment (the container).
- An orchestration and scheduling controller (which can be a collection of multiple tools).
- A repository for the container images or code to execute.
- Together, these are the place to run things, the things to run, and the management system to tie them together.

Regardless of the technology platform, container security includes:

- *Assuring the security of the underlying physical infrastructure (compute, network, storage).* This is no different than any other form of virtualization, but it now extends into the underlying operating system where the container's execution environment runs.
- *Assuring the security of the management plane,* which in this case are the orchestrator and the scheduler.
- *Properly securing the image repository.* The image repository should be in a secure location with appropriate access controls configured. This is both to prevent loss or unapproved modification of container images and definition files, as well as to forestall leaks of sensitive data through unapproved access to the files. Containers run so easily that it's also important that images are only able to deploy in the right security context.
- *Building security into the tasks/code running inside the container.* It's still possible to run vulnerable software inside a container and, in some cases this could expose the shared operating system or data from other containers. For example, it is possible to configure some containers to allow not merely access to the container's data on the file system but also root file system access. Allowing too much network access is also a possibility. These are all specific to the particular container platform and thus require securely configuring both the container environment *and* the images/container configurations themselves.

Containers are rapidly evolving, which complicates some aspects of security, but doesn't mean that they are inherently insecure.

Containers don't necessarily provide full security isolation, but they do provide task segregation. That said, virtual machines typically do provide security isolation. Thus you can put tasks of equivalent security context on the same set of physical or virtual hosts in order to provide greater security segregation.

Container management systems and image repositories also have different security capabilities, based on which products you use. Security should learn and understand the capabilities of the products they need to support. Products should, at a minimum, support role-based access controls and strong authentication. They should also support secure configurations, such as isolating file system, process, and network access.



A deep understanding of container security relies on a deep understanding of operating system internals, such as namespaces, network port mapping, memory, and storage access.

Different host operating systems and container technologies offer different security capabilities. This assessment should be included in any container platform selection process.

One key area to secure is which images/tasks/code are allowed into a particular execution environment. A secure repository with proper container management and scheduling will enable this.

## 8.2 Recommendations

- Cloud providers should:
  - Inherently secure any underlying physical infrastructure used for virtualization.
  - Focus on assuring security isolation between tenants.
  - Provide sufficient security capabilities at the virtualization layers to allow cloud users to properly secure their assets.
  - Strongly defend the physical infrastructure and virtualization platforms from attack or internal compromise.
  - Implement all customer-managed virtualization features with a secure-by-default configuration.
  - Specific priorities:
    - Compute
      - Use secure hypervisors and implement a patch management process to keep them up to date.
      - Configure hypervisors to isolate virtual machines from each other.
      - Implement internal processes and technical security controls to prevent admin/non-tenant access to running VMs or volatile memory.
    - Network
      - Implement essential perimeter security defenses to protect the underlying networks from attack and, wherever possible, to detect and prevent attacks against consumers at the physical level, as well as at any virtual network layers that they can't directly protect themselves.
      - Assure isolation between virtual networks, even if those networks are all controlled by the same consumer.
        - Unless the consumer deliberately connects the separate virtual networks.
      - Implement internal security controls and policies to prevent both modification of consumer networks and monitoring of traffic without approval or outside contractual agreements.
    - Storage
      - Encrypt any underlying physical storage, if it is not already encrypted at another level, to prevent data exposure during drive replacements.
      - Isolate encryption from data-management functions to prevent unapproved access to customer data.

- Cloud users should:
  - Ensure they understand the capabilities offered by their cloud providers as well as any security gaps.
  - Properly configure virtualization services in accordance with the guidance from the cloud provider and other industry best practices.
    - The bulk of fundamental virtualization security falls on the cloud provider, which is why most of the security recommendations for cloud users are covered in the other domains of this Guidance.
  - For containers:
    - Understand the security isolation capabilities of both the chosen container platform and underlying operating system then choose the appropriate configuration.
    - Use physical or virtual machines to provide container isolation and group containers of the same security contexts on the same physical and/or virtual hosts.
    - Ensure that only approved, known, and secure container images or code can be deployed.
    - Appropriately secure the container orchestration/management and scheduler software stack(s).
    - Implement appropriate role-based access controls and strong authentication for all container and repository management.



# DOMAIN 9

# Incident Response



## 9.0 Introduction

Incident Response (IR) is a critical facet of any information security program. Preventive security controls have proven unable to completely eliminate the possibility that critical data could be compromised. Most organizations have some sort of IR plan to govern how they will investigate an attack, but as the cloud presents distinct differences in both access to forensic data and governance, organizations must consider how their IR processes will change.

This domain seeks to identify those gaps pertinent to IR that are created by the unique characteristics of cloud computing. Security professionals may use this as a reference when developing response plans and conducting other activities during the preparation phase of the IR lifecycle. This domain is organized in accord with the commonly accepted Incident Response Lifecycle as described in the National Institute of Standards and Technology Computer Security Incident Handling Guide (NIST 800-61rev2 08/2012) [1]. Other international standard frameworks for incident response include ISO/IEC 27035 and the ENISA Strategies for incident response and cyber crisis cooperation.

After describing the Incident Response Lifecycle, as laid out in NIST 800-61rev2, each subsequent section addresses a phase of the lifecycle and explores the potential considerations for responders as they work in a cloud environment.

# 9.1 Overview

## 9.1.1 Incident Response Lifecycle

The Incident Response Lifecycle is defined in the NIST 800-61rev2 document. It includes the following phases and major activities:



*The Incident Response Lifecycle*

- Preparation: "Establishing an incident response capability so that the organization is ready to respond to incidents."
  - Process to handle the incidents.
  - Handler communications and facilities.
  - Incident analysis hardware and software.
  - Internal documentation (port lists, asset lists, network diagrams, current baselines of network traffic).
  - Identifying training.
  - Evaluating infrastructure by proactive scanning and network monitoring, vulnerability assessments, and performing risk assessments.
  - Subscribing to third-party threat intelligence services.
- Detection and Analysis
  - Alerts [endpoint protection, network security monitoring, host monitoring, account creation, privilege escalation, other indicators of compromise, SIEM, security analytics (baseline and anomaly detection), and user behavior analytics].
  - Validate alerts (reducing false positives) and escalation.
  - Estimate the scope of the incident.
  - Assign an Incident Manager who will coordinate further actions.
  - Designate a person who will communicate the incident containment and recovery status to senior management.
  - Build a timeline of the attack.
  - Determine the extent of the potential data loss.
  - Notification and coordination activities.
  - Containment, eradication and recovery
  - Containment: Taking systems offline. Considerations for data loss versus service availability. Ensuring systems don't destroy themselves upon detection.
  - Eradication and recovery: Clean up compromised devices and restore systems to normal operation. Confirm systems are functioning properly. Deploy controls to prevent similar incidents.
  - Documenting the incident and gathering evidence (chain of custody).

- Post-mortem
  - What could have been done better? Could the attack have been detected sooner? What additional data would have been helpful to isolate the attack faster? Does the IR process need to change? If so, how?

## **9.1.2 How the Cloud Impacts IR**

Each of the phases of the lifecycle is affected to different degrees by a cloud deployment. Some of these are similar to any incident response in an outsourced environment where you need to coordinate with a third party. Other differences are more specific to the abstracted and automated nature of cloud.

### **9.1.2.1 Preparation**

When preparing for cloud incident response, here are some major considerations:

- *SLAs and Governance:* Any incident using a public cloud or hosted provider requires an understanding of service level agreements (SLAs), and likely coordination with the cloud provider. Keep in mind that, depending on your relationship with the provider, you may not have direct points of contact and might be limited to whatever is offered through standard support. A custom private cloud in a third-party data center will have a very different relationship than signing up through a website and clicking through a license agreement for a new SaaS application.

Key questions include: What does your organization do? What is the cloud service provider (CSP) responsible for? Who are the points of contact? What are the response time expectations? What are the escalation procedures? Do you have out-of-band communication procedures (in case networks are impacted)? How do the hand-offs work? What data are you going to have access to?

Be sure to test the process with the CSP if possible. Validate that escalations and roles/responsibilities are clear. Ensure the CSP has contacts to notify you of incidents they detect, and that such notifications are integrated into your process. For click-through services, notifications will likely be sent to your registration email address; these should be controlled by the enterprise and monitored continuously. Ensure that you have contacts, including out-of-band methods, for your CSP and that you test them.

- *IaaS/PaaS vs. SaaS:* In a multitenant environment, how can data specific to your cloud be provided for investigation? For each major service you should understand and document what data and logs will be available in an incident. Don't assume you can contact a provider after the fact and collect data that isn't normally available.
- *"Cloud jump kit."* These are the tools needed to investigate in a remote location (as with cloud-based resources). For example, do you have tools to collect logs and metadata from the cloud platform? Do you have the ability to interpret the information? How do you obtain images of running virtual machines and what kind of data do you have access to: disk storage or volatile memory?

- Architect the cloud environment for faster detection, investigation, and response (containment and recoverability). This means ensuring you have the proper configuration and architecture to support incident response:
  - Enable instrumentation, such as cloud API logs, and ensure that they feed to a secure location that's available to investigators in case of an incident.
  - Utilize isolation to ensure that attacks cannot spread and compromise the entire application.
  - Use immutable servers when possible. If an issue is detected, move workloads from compromised device onto a new instance in a known-good state. Employ a greater focus on file integrity monitoring and configuration management.
  - Implement application stack maps to understand where data is going to reside in order to factor in geographic differences in monitoring and data capture.
  - It can be very helpful to perform threat modeling and tabletop exercises to determine the most effective means of containment for different types of attacks on different components in the cloud stack.
  - This should include differences between responses for IaaS/PaaS/SaaS.

#### 9.1.2.2 Detection and Analysis

Detection and analysis in a cloud environment may look nearly the same (for IaaS) and quite different (for SaaS). In all cases, the monitoring scope must cover the cloud's management plane, not merely the deployed assets.

You may be able to leverage in-cloud monitoring and alerts that can kick off an automated IR workflow in order to speed up the response process. Some cloud providers offer these features for their platforms, and there are also some third-party monitoring options available. These may not be security-specific: Many cloud platforms (IaaS and possibly PaaS) expose a variety of real-time and near-real-time monitoring metrics for performance and operational reasons. But security may also be able to leverage these for security needs.

Cloud platforms also offer a variety of logs, which can sometimes be integrated into existing security operations/monitoring. These could range from operational logs to full logging of all API calls or management activity. Keep in mind that they are not available on all providers; you tend to see them more with IaaS and PaaS than SaaS. When log feeds aren't available you may be able to use the cloud console as a means to identify environment/configuration changes.

*Data sources* for cloud incidents can be quite different from those used in incident response for traditional computing. There is significant overlap, such as system logs, but there are differences in terms of how data can be collected and in terms of new sources, such as feeds from the cloud management plane.

As mentioned, cloud platform logs may be an option, but they are not universally available. Ideally they should show all management-plane activity. It's important to understand what is logged and the gaps that could affect incident analysis. Is all management activity recorded? Do they include automated system activities (like auto-scaling) or cloud provider management activities? In the case of a serious incident, providers may have other logs that are not normally available to customers.



One challenge in collecting information may be limited network visibility. Network logs from a cloud provider will tend to be flow records, but not full packet capture.

Where there are gaps you can sometimes instrument the technology stack with your own logging. This can work within instances, containers, and application code in order to gain telemetry important for the investigation. Pay particular attention to PaaS and serverless application architectures; you will likely need to add custom application-level logging.

External threat intelligence may also be useful, as it is with on-premises incident response, in order to help identify indicators of compromise and to get adversary information.

Be aware that there are potential challenges when the information that is provided by a CSP faces chain of custody questions. There are no reliable precedents established at this point.

*Forensics and investigative support* will also need to adapt, beyond understanding changes to data sources.

Always factor in what the CSP can provide and whether it meets chain of custody requirements. Not every incident will result in legal action, but it's important to work with your legal team to understand the lines and where you could end up having chain of custody issues.

There is a greater need to automate many of the forensic/investigation processes in cloud environments, because of their dynamic and higher-velocity nature. For example, evidence could be lost due to a normal auto-scaling activity or if an administrator decides to terminate a virtual machine involved in an investigation. Some examples of tasks you can automate include:

- Snapshotting the storage of the virtual machine.
- Capturing any metadata at the time of alert, so that the analysis can happen based on what the infrastructure looked like at that time.
- If your provider supports it, “pausing” the virtual machine, which will save the volatile memory state.

You can also leverage the capabilities of the cloud platform to determine the extent of the potential compromise:

- Analyze network flows to check if network isolation held up. You can also use API calls to snapshot the network and the virtual firewall rules state, which could give you an accurate picture of the entire stack at the time of the incident.
- Examine configuration data to check if other similar instances were potentially exposed in the same attack.
- Review data access logs (for cloud-based storage, if available) and management plane logs to see if the incident affected or spanned into the cloud platform.
- Serverless and PaaS-based architectures will require additional correlation across the cloud platform and any self-generated application logs.



### 9.1.2.3 Containment, Eradication and Recovery

Always start by ensuring the cloud management plane/metastructure is free of an attacker. This will often involve invoking break-glass procedures to access the root or master credentials for the cloud account, in order to ensure that attacker activity isn't being masked or hidden from lower-level administrator accounts. Remember: You can't contain an attack if the attacker is still in the management plane. Attacks on cloud assets, such as virtual machines, may sometimes reveal management plane credentials that are then used to bridge into a wider, more serious attack.

The cloud often provides a lot more flexibility in this phase of the response, especially for IaaS. Software-defined infrastructure allows you to quickly rebuild from scratch in a clean environment, and, for more isolated attacks, inherent cloud characteristics—such as auto-scale groups, API calls for changing virtual network or machine configurations, and snapshots—can speed quarantine, eradication, and recovery processes. For example, on many platforms you can instantly quarantine virtual machines by moving the instance out of the auto-scale group, isolating it with virtual firewalls, and replacing it.

This also means there's no need to immediately "eradicate" the attacker before you identify their exploit mechanisms and the scope of the breach, since the new infrastructure/instances are clean; instead, you can simply isolate them. However, you still need to ensure the exploit path is closed and can't be used to infiltrate other production assets. If there is concern that the management plane is breached, be sure to confirm that the templates or configurations for new infrastructure/applications have not been compromised.

That said, these capabilities are not always universal: With SaaS and some PaaS you may be very limited and will thus need to rely more on the cloud provider.

### 9.1.2.4 Post-mortem

As with any attack, work with the internal response team and provider to figure what worked and what didn't, then pinpoint any areas for improvement. Pay particular attention to the limitations in the data collected and figure out how to address the issues moving forward.

It is hard to change SLAs, but if the agreed-upon response time, data, or other support wasn't sufficient, go back and try to renegotiate.

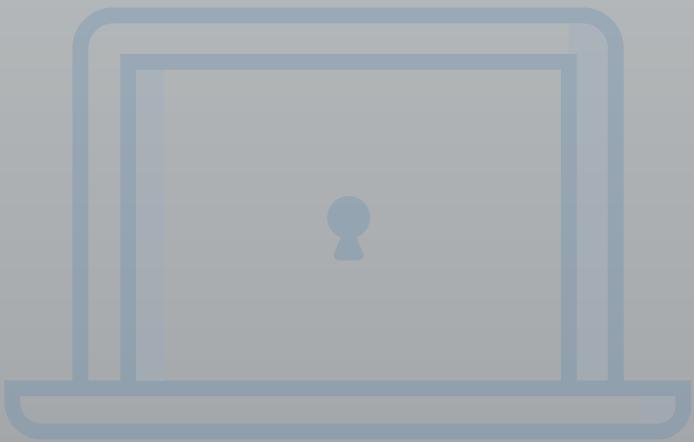
## 9.2 Recommendations

- SLAs and setting expectations around what the customer does versus what the provider does are the most important aspects of incident response for cloud-based resources. Clear communication of roles/responsibilities and practicing the response and hand-offs are critical.
- Cloud customers must set up proper communication paths with the provider that can be utilized in the event of an incident. Existing open standards can facilitate incident communication.
- Cloud customers must understand the content and format of data that the cloud provider will supply for analysis purposes and evaluate whether the available forensics data satisfies legal chain of custody requirements.
- Cloud customers should also embrace continuous and serverless monitoring of cloud-based resources to detect potential issues earlier than in traditional data centers.
  - Data sources should be stored or copied into locations that maintain availability during incidents.
  - If needed and possible, they should also be handled to maintain a proper chain of custody.
- Cloud-based applications should leverage automation and orchestration to streamline and accelerate the response, including containment and recovery.
- For each cloud service provider used, the approach to detecting and handling incidents involving the resources hosted at that provider must be planned and described in the enterprise incident response plan.
- The SLA with each cloud service provider must guarantee support for the incident handling required for the effective execution of the enterprise incident response plan. This must cover each stage of the incident handling process: detection, analysis, containment, eradication, and recovery.
- Testing will be conducted at least annually or whenever there are significant changes to the application architecture. Customers should seek to integrate their testing procedures with that of their provider (and other partners) to the greatest extent possible.



# DOMAIN 10

# Application Security



## 10.0 Introduction

Application security encompasses an incredibly complex and large body of knowledge: everything from early design and threat modeling to maintaining and defending production applications.

Application security is also evolving at an incredibly rapid pace as the practice of application development continues to progress and embrace new processes, patterns, and technologies. Cloud computing is one of the biggest drivers of these advancements and that results in corresponding pressure to evolve the state of application security, in order to ensure that this progress continues as safely as possible.

This section of the guidance is intended for software development and IT teams who want to securely build and deploy applications in cloud computing environments, specifically PaaS and IaaS. (Many of the techniques in this section are used to underpin secure SaaS applications as well.) It focuses on:

- How application security differs in cloud computing.
- Reviewing secure software development basics and how those change in the cloud.
- Leveraging cloud capabilities for more secure cloud applications.

We can't cover all possible development and deployment options—even just the ones directly related to cloud computing—so the goal is to focus on significant areas that should help guide security in the majority of situations. This domain also introduces security fundamentals for DevOps, which is rapidly emerging as a dominant force in cloud-based application development.

Cloud computing mostly brings security benefits to applications, but as with most areas of cloud technology, it does require commensurate changes to existing practices, processes, and technologies that were not designed to operate in the cloud. At a high level, this balance of opportunities and challenges includes:

### *Opportunities*

- *Higher baseline security.* Cloud providers, especially major IaaS and PaaS providers, have



significant economic incentives to maintain higher baseline security than most organizations. In a cloud environment, major baseline security failures completely undermine the trust that a public cloud provider needs in order to maintain relationships with its customer base. Cloud providers are also subject to a wider range of security requirements in order to meet all the regulatory and industry compliance baselines needed to attract customers from those verticals. These combine to strongly motivate cloud providers to maintain extremely high levels of security.

- *Responsiveness.* APIs and automation provide extensive flexibility to build more responsive security programs at a lower cost than in traditional infrastructure. For example, changing firewall rules or deploying new servers with updated code can be handled with a few API calls or through automation.
- *Isolated environments.* Cloud applications can also leverage virtual networks and other structures, including PaaS, for hyper-segregated environments. For example, it is possible, at no additional cost, to deploy multiple application stacks on entirely separate virtual networks, eliminating the ability for an attacker to use one compromised application to attack others behind the perimeter firewalls.
- *Independent virtual machines.* Security is further enhanced by the use of micro-service architectures. Since cloud doesn't require the consumer to optimize the use of physical servers, a requirement that often results in deploying multiple application components and services on a single system, developers can instead deploy more, smaller virtual machines, each dedicated to a function or service. This reduces the attack surface of the individual virtual machines and supports more granular security controls.
- *Elasticity.* Elasticity enables greater use of immutable infrastructure. When using elasticity tools like auto-scale groups, each production system is launched dynamically based on a baseline image, and may be automatically deprovisioned without human interaction. Thus, core operational requirements mean you never want to allow an administrator to log into a system and make changes, since they will be lost during a normal auto-scale activity. This enables the use of immutable servers, where remote administration is completely disabled. We describe immutable servers and infrastructure in more detail in Domain 7.
- *DevOps.* DevOps is a new application development methodology and philosophy focused on automation of application development and deployment. DevOps opens up many opportunities for security to improve code hardening, change management, and production application security, and even to enhance security operations in general.
- *Unified interface.* A unified interface (management interface and APIs) for infrastructure and application services (when using PaaS) provides a more comprehensive view and better management compared to the traditional disparate systems and devices (load balancers, servers, network devices, firewalls, ACLs, etc.), which are often managed by different groups. This creates opportunities to reduce security failures due to lack of communication or full-stack visibility.

## Challenges

- *Limited detailed visibility.* Visibility and the availability of monitoring and logging are impacted, requiring new approaches to gathering security-related data. This is especially true when using PaaS, where commonly available logs, such as system or network logs, are often no longer accessible to the cloud user.

- *Increased application scope.* The management plane/metastructure security directly affects the security of any applications associated with that cloud account. Developers and operations will also likely need access to the management plane, as opposed to always going through a different team. Data and sensitive information is also potentially exposable within the management plane. Lastly, modern cloud applications often connect with the management plane to trigger a variety of automated actions, especially when PaaS is involved. For all those reasons, management plane security is now within scope of the application's security and a failure on either side could bridge into the other.
- *Changing threat models.* The cloud provider relationship and the shared security model will need to be included in the threat model, as well as in any operational and incident response plans. Threat models also need to adapt to reflect the technical differences of the cloud provider or platform in use.
- *Reduced transparency.* There may be less transparency as to what is going on within the application, especially as it integrates with external services. For example, you rarely know the entire set of security controls for an external PaaS service integrated with your application.

Overall, there will be changes to application security due to the shared security model. Some of these are directly tied to governance and operations, but there are many more in terms of how you think and plan for the application's security.

## 10.1 Overview

Due to the broad nature of application security and the many different skill sets and roles involved in an effective application security program, this domain is broken into the following major areas:

- *The Secure Software Development Lifecycle (SSDLC):* How cloud computing affects application security, from design to deployment.
- *Design and Architecture:* Trends in designing applications for cloud computing that affect and can even improve security.
- *DevOps and Continuous Integration/Continuous Deployment (CI/CD):* DevOps and CI/CD are very frequently used in both the development and deployment of cloud applications, and are quickly becoming the dominant models. They bring new security considerations, and again, opportunities to improve security over more manual development and deployment patterns like waterfall.

### 10.1.1 Introduction to the Secure Software Development Lifecycle and Cloud Computing

The SSDLC describes a series of security activities during all phases of application development, deployment, and operations. There are multiple frameworks used in the industry, including:

- Microsoft's Security Development Lifecycle
- NIST 800-64
- ISO/IEC 27034
- Other organizations, including Open Web Application Security Project (OWASP) and a variety of



application security vendors, also publish their own lifecycle and security activities guidance.

Due to the range of frameworks and differences in terminology, the Cloud Security Alliance breaks these into larger “meta-phases” to help describe the relatively standard set of activities seen across the frameworks. These aren’t meant to replace the formal methodologies, but merely provide a descriptive model that we can use to address the major activities, independent of whatever lifecycle an organization will standardize on.

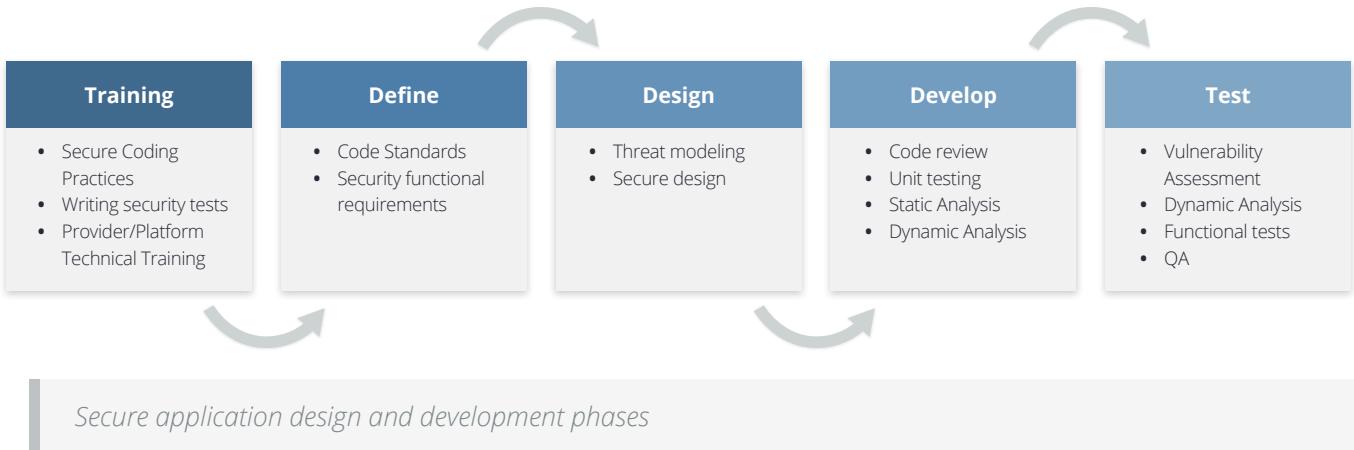
- *Secure Design and Development:* From training and developing organization-wide standards to actually writing and testing code.
- *Secure Deployment:* The security and testing activities when moving code from an isolated development environment into production.
- *Secure Operations:* Securing and maintaining production applications, including external defenses such as Web Application Firewalls (WAF) and ongoing vulnerability assessments.

Cloud computing affects every phase of the SSDLC, regardless of which particular SSDLC you use. This is a direct result of the abstraction and automation of cloud computing, combined with (in the public cloud) a greater reliance on an external provider. Specifically:

- The shared responsibility model means there is always some reliance on the cloud provider for some aspects of security, even in a very bare-bones IaaS-based application. The more you adopt PaaS and provider-specific features, the greater the split in security responsibilities. It could be as simple as using a cloud load balancer, which the provider is completely responsible for keeping secure but the cloud user is responsible for configuring and using properly.
- There are large changes in visibility and control, as discussed in nearly every domain of this Guidance. When running mostly on IaaS it might just be a lack of network logs, but as you move into PaaS it may mean a loss of server and service logs. And, it will all vary based on provider and technology.
- Different cloud providers have different capabilities in terms of features, services, and security, which must be accounted for in the overall application security plan.
- The management plane and metastructure may now be within the application security scope, especially when the application components communicate directly with the cloud service.
- There are new and different architectural options, especially, again, as you consume PaaS.
- The rise and impact of DevOps, which we cover later in this Domain.

## **10.1.2 Secure Design and Development**

There are five main phases in secure application design and development, all of which are affected by cloud computing:



*Training:* Three different roles will require two new categories of training. Development, operations, and security should all receive additional training on cloud security fundamentals (which are not provider specific), as well as appropriate technical security training on any specific cloud providers and platforms used on their projects. There is typically greater developer and operations involvement in directly architecting and managing the cloud infrastructure, so baseline security training that's specific to the tools they will use is essential.

*Define:* The cloud user determines the approved architectures or features/tools for the provider, security standards, and other requirements. This might be tightly coupled to compliance requirements, listing, for example, what kind of data is allowed onto which cloud services (including individual services within a larger provider). At this step the deployment processes should also be defined, although that is sometimes finalized later in a project. Security standards should include the initial entitlements for who is allowed to manage which services in the cloud provider, which is often independent of the actual application architecture. It should also include pre-approved tools, technologies, configurations, and even design patterns.

*Design:* During the application design process, especially when PaaS is involved, the focus for security in cloud is on architecture, the cloud provider's baseline capabilities, cloud provider features, and automating and managing security for deployment and operations. We find that there are often significant security benefits to integrating security into the application architecture since there are opportunities to leverage the provider's own security capabilities. For example, inserting a serverless load balancer or message queue could completely block certain network attack paths. This is also where you perform threat modeling, which must also be cloud and provider/platform specific.

*Develop:* Developers may need a development environment with administrative access to the cloud management plane so that they can configure networks, services, and other settings. This should never be a production environment or hold production data. Developers will also likely use a CI/CD pipeline, which must be secured—especially the code repository. If PaaS is used, then



developers should build logging into their application to compensate, as much as possible, for any loss of network, system, or service logs.

*Test:* Security testing should be integrated into the deployment process and pipeline. Testing tends to span this and the Secure Deployment phase, but leans towards security unit tests, security functional tests, Static Application Security Testing (SAST), and Dynamic Application Security Testing (DAST). Due to the overlap, we cover the cloud considerations in more depth in the next section. Organizations should also rely more on automated testing in cloud. Infrastructure is more often in scope for application testing due to “infrastructure as code,” where the infrastructure itself is defined and implemented through templates and automation. As part of security testing, consider requiring flagging features for security-sensitive capabilities that may require deeper security review, such as authentication and encryption code.

### **10.1.3 Secure Deployment**

Since deployment automation tends to be more prominent in cloud environments, it often includes certain security activities that could also be implemented in the Design and Development phase. Automated security testing is very frequently integrated into the deployment pipeline and performed outside of direct developer control. This is in and of itself a departure from many on-premises development efforts, but the testing itself also needs to be adapted for cloud computing.

There are multiple kinds of application security tests that could be potentially integrated into development and deployment:

*Code Review:* This is a manual activity that's not necessarily integrated into automated testing, but the CI/CD pipeline might impose a manual gate. The review itself doesn't necessarily change for cloud, but there are specific areas that need additional attention. Any application communication with the management plane (e.g., API calls to the cloud service, some of which can alter the infrastructure) should be scrutinized, especially early in the project. Aside from looking at the code itself, the security team can focus on ensuring that only the least privilege entitlements are enabled for that part of the application and then validate them with the management plane configuration. Anything related to authentication and encryption is also important for additional review. The deployment process can then be automated to notify security if there are any modifications to these portions of code that might require manual approval, or just after-the-fact change review.

*Unit testing, regression testing, and functional tests:* These are the standard tests used by developers in their normal processes. Security testing can and should be integrated in these to ensure that the security features in the application continue to function as expected. The tests themselves will likely need to be updated to account for running in the cloud, including any API calls.

*Static Application Security Testing (SAST):* On top of the normal range of tests, these should ideally incorporate checks on API calls to the cloud service. They should also look for any static embedded credentials for those API calls, which is a growing problem.

*Dynamic Application Security Testing (DAST):* DAST tests running applications and includes tests



such as web vulnerability testing and fuzzing. Due to the terms of service with the cloud provider DAST may be limited and/or require pre-testing permission from the provider. With cloud and automated deployment pipelines it is possible to stand up entirely functional test environments using infrastructure as code and then perform deep assessments before approving changes for production.

#### 10.1.3.1 Impact on Vulnerability Assessment

Vulnerability assessment can be integrated into CI/CD pipelines and implemented in cloud fairly easily, but it nearly always requires compliance with the provider's terms of service.

There are two specific patterns we commonly see. The first is running full assessments against images or containers as part of the pipeline in a special testing area of the cloud (a segment of a virtual network) that you define for this purpose. The image is only approved for production deployments if it passes this test. We see a similar pattern used to test entire infrastructures by building a test environment using infrastructure as code.

In both cases production is tested less, or not at all, since it should be immutable and exactly resemble the test environment (both are based on the same definition files). Organizations can also use host-based vulnerability assessment tools, which run locally in a virtual machine and thus do not require coordination with or permission of the cloud provider.

#### 10.1.3.2 Impact on Penetration Testing

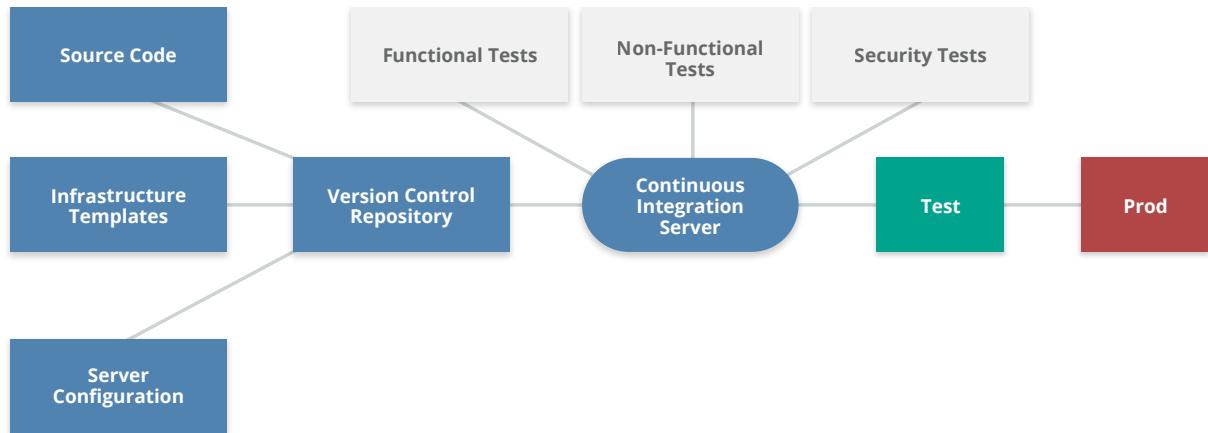
As with vulnerability assessment there will almost certainly be limits on performing penetration tests without the permission of the cloud provider. The CSA recommends adapting penetration testing for cloud using the following guidelines:

- Use a testing firm that has experience on the cloud provider where the application is deployed.
- Include developers and cloud administrators within the scope of the test. Many cloud breaches attack those who maintain the cloud, not the application on the cloud itself. This includes the cloud management plane.
- If the application is a multitenant app, then allow the penetration testers authorized access as a tenant to see if they can compromise the tenancy isolation and use their access to break into another tenant's environment or data.

#### 10.1.3.3 Deployment Pipeline Security

CI/CD pipelines can enhance security through support of immutable infrastructure (fewer manual changes to production environments), automating security testing, and extensive logging of application and infrastructure changes when those changes run through the pipeline. When configured properly, logs can track every code, infrastructure, and configuration change and tie them back to whoever submitted the change and whoever approved it; they will also include any testing results.

The pipeline itself needs to be tightly secured. Consider hosting pipelines in a dedicated cloud environment with very limited access to the cloud or the infrastructure hosting the pipeline components.



*A continuous deployment pipeline.*

#### 10.1.3.4 Impact of Infrastructure as Code and Immutable

In multiple places we refer to infrastructure as code. Due to the virtual and software-defined nature of cloud it is often possible to define entire environments using templates that are translated by tools (either the provider's or third party) into API calls that automatically build the environment. A basic example is building a server configuration from a template. More complex implementations can build entire cloud application stacks, down to the network configuration and identity management.

Since these environments are built automatically from a set of source file definitions, they can also be immutable. If the system or environment is built automatically from a template, likely from a CI/CD pipeline, then any changes made in production will be overwritten by the next code or template change. The production environment can thus be locked down much more tightly than is normally possible in a non-cloud application deployment, where much of the infrastructure is configured manually to a specification. When security is properly engaged, the use of infrastructure as code and immutable deployments can significantly improve security.

#### 10.1.4 Secure Operations

When an application is deployed into production, security activities continue. Many of these are covered in other areas throughout this Guidance, especially in Domain 7 (Infrastructure), Domain 8 (Containers), Domain 11 (Data), and Domain 12 (Identity and Access Management). This section contains additional guidance that more directly applies to applications:

- The management plane for production environments should be much more tightly locked down than those for development. As previously mentioned, if the application directly accesses the management plane for the environment where it is hosted, then those privileges should be scoped to the least possible required. We recommend using multiple sets of credentials for each application service in order to further compartmentalize entitlements.
- Even when using immutable infrastructure, the production environment should still be actively monitored for changes and deviations from approved baselines. This can and should be



automated through code (or tools) that make API calls to the cloud in order to regularly assess configuration state.

On some cloud platforms it may be possible to use built-in assessment and configuration management features. It may also be possible to automatically remediate unapproved changes, depending on the platform and the nature of the change. For example, code can automatically revert any firewall rule changes that weren't approved by security.

- Even after deployment, and even using immutable infrastructure, don't neglect ongoing application testing and assessment. In public cloud scenarios, this will likely require coordination with or permission of the cloud provider to avoid violating terms of service, just as with any other vulnerability assessment.
- Change management doesn't just include the application, but also any infrastructure and the cloud management plane.

For information on incident response, see Domain 9; for more on business continuity and management plane security, see Domain 6.

### **10.1.5 How Cloud Impacts Application Design and Architectures**

The very nature of cloud is already creating changes in preferred application designs, architectures, and patterns. Some of these have nothing directly to do with security, but the following trends offer opportunities to reduce common security issues:

- *Segregation by default:* Applications can easily be run in their own isolated cloud environments. Depending on the provider, this could be a separate virtual network or account/sub-account. Using accounts or sub-account structures offers the benefit of enabling management plane segregation. The organization can open up wider rights in development accounts while running highly-restrictive production accounts.
- *Immutable infrastructure:* As mentioned, immutable infrastructure is becoming increasingly common in cloud, for operational reasons. Security can extend these benefits by disabling remote logins to immutable servers/containers, adding file integrity monitoring, and integrating immutable techniques into incident recovery plans.
- *Increased use of micro-services:* In cloud computing, it is easier to segregate out different services onto different servers (or containers), since, for one thing, you no longer need to maximize utilization of physical servers and, for another, auto-scale groups can assure application scalability even when using fleets of smaller computer nodes for workloads. Since each node does less, it's easier to lock down and minimize the services running on it. While this improves the security of each workload (when used correctly), it does add some overhead to secure the communications between all the micro-services and ensure that any service discovery, scheduling, and routing is also configured securely.
- *PaaS and "serverless" architectures:* With PaaS and "serverless" setups (running workloads directly on the cloud provider's platform, where you don't manage the underlying services and operating system) there is great potential for dramatically reducing the attack surface. This is only if the cloud provider takes responsibility for the security of the platform/serverless setup and meets your

requirements.

Serverless can bring a few advantages. First, there are large economic incentives for the provider to maintain extremely high security levels and keep their environment up to date. This removes the day-to-day responsibility for keeping these secure from the cloud user, but never obviates their ultimate accountability for security. Working with a trusted cloud provider with a strong track record is critical.

Next, the serverless platforms may run on the provider's network with communications to the consumer's components through API or HTTPS traffic. This removes direct network attack paths, even if an attacker compromises a server or container. The attacker is limited to attempting API calls or HTTPS traffic and can't port scan, identify other servers, or use other common techniques.

- *Software-defined security*: Security teams can leverage all the same tools and technologies to automate many security operations, even integrating them with the application stack. Some examples include automating cloud incident response, automating dynamic changes to entitlements, and remediation of unapproved infrastructure changes.
- *Event driven security*: Certain cloud providers support event-driven code execution. In these cases, the management plane detects various activities—such as a file being uploaded to a designated object storage location or a configuration change to the network or identity management—which can in turn trigger code execution through a notification message, or via serverless hosted code. Security can define events for security actions and use the event-driven capabilities to trigger automated notification, assessment, remediation, or other security processes.

### **10.1.6 Additional Considerations for Cloud Providers**

Cloud providers of all service models need to pay extra attention to certain aspects of their application services that could cause very significant problems for their customers if there are security issues:

- APIs and web services need to be extensively hardened and assume attacks from both authenticated and unauthenticated adversaries. This includes using industry-standard authentication designed specifically for APIs.
- APIs should be monitored for abuse and unusual activity.
- The service should undergo extensive design and testing to prevent attacks or inappropriate/accidental cross-tenant access.

### **10.1.7 The Rise and Role of DevOps**

DevOps refers to the deeper integration of development and operations teams through better collaboration and communications, with a heavy focus on automating application deployment and infrastructure operations. There are multiple definitions, but the overall idea consists of a culture, philosophy, processes, and tools.

At the core is the combination of Continuous Integration and/or Continuous Delivery (CI/CD) through automated deployment pipelines, and the use of programmatic automation tools to better manage infrastructure. DevOps is not exclusive to cloud, but as discussed it is highly attuned to cloud and is growing to become the dominant cloud application delivery model.



#### 10.1.7.1 Security Implications and Advantages

- *Standardization:* With DevOps, anything that goes into production is created by the CI/CD pipeline on approved code and configuration templates. Dev/Test/Prod are all based on the exact same source files, which eliminates any deviation from known-good standards.
- *Automated testing:* As discussed, a wide variety of security testing can be integrated into the CI/CD pipeline, with manual testing added as needed to supplement.
- *Immutable:* CI/CD pipelines can produce master images for virtual machines, containers, and infrastructure stacks very quickly and reliably. This enables automated deployments and immutable infrastructure.
- *Improved auditing and change management:* CI/CD pipelines can track everything, down to individual character changes in source files that are tied to the person submitting the change, with the entire history of the application stack (including infrastructure) stored in a version control repository. This offers considerable audit and change-tracking benefits.
- *SecDevOps/DevSecOps and Rugged DevOps:* These two terms are emerging to describe the integration of security activities into DevOps. SecDevOps/DevSecOps sometimes refers to the use of DevOps automation techniques to improve security operations. Rugged DevOps refers to integration of security testing into the application development process to produce harder, more secure, and more resilient applications.

## 10.2 Recommendations

- Understand the security capabilities of your cloud providers. Not merely their baseline, but the various platforms and services.
- Build security into the initial design process. Cloud deployments are more often greenfield, creating new opportunities to engage security early.
- Even if you don't have a formal SDLC, consider moving to continuous deployment and automating security into the deployment pipeline.
- Threat modeling, SAST, and DAST (with fuzzing) should all be integrated. Testing should be configured to work in the cloud environment, but also to test for concerns specific to cloud platforms, such as stored API credentials.
- Understand the new architectural options and requirements in the cloud. Update your security policies and standards to support them, and don't merely attempt to enforce existing standards on an entirely different computing model.
- Integrate security testing into the deployment process.
- Use software-defined security to automate security controls.
- Use event-driven security, when available, to automate detection and remediation of security issues.
- Use different cloud environments to better segregate management plane access and provide developers the freedom they need to configure development environments, while also locking down production environments.



# DOMAIN 11

# Data Security and Encryption



## 11.0 Introduction

Data security is a key enforcement tool for information and data governance. As with all areas of cloud security, its use should be risk-based since it is not appropriate to secure everything equally.

This is true for data security overall, regardless of whether the cloud is involved. However, many organizations aren't as accustomed to trusting large amounts of their sensitive data—if not all of it—to a third party, or mixing all their internal data into a shared resource pool. As such, the instinct may be to set a blanket security policy for “anything in the cloud” instead of sticking with a risk-based approach, which will be far more secure and cost effective.

For example, encrypting everything in SaaS because you don't trust that provider at all likely means that you shouldn't be using the provider in the first place. But encrypting everything is not a cure-all and may lead to a false sense of security, e.g., encrypting data traffic without ensuring the security of the devices themselves.

By some perspectives information security is data security, but for our purposes this domain will focus on those controls related to securing the data itself, of which encryption is one of the most important.

## 11.1 Overview

### 11.1.1 Data Security Controls

Data security controls tend to fall into three buckets. We cover all of these in this section:

- Controlling what data goes into the cloud (and where).
- Protecting and managing the data in the cloud. The key controls and processes are:
  - Access controls
  - Encryption
  - Architecture

- Monitoring/alerting (of usage, configuration, lifecycle state, etc.)
- Additional controls, including those related to the specific product/service/platform of your cloud provider, data loss prevention, and enterprise rights management.
- Enforcing information lifecycle management security.
  - Managing data location/residency.
  - Ensuring compliance, including audit artifacts (logs, configurations).
  - Backups and business continuity, which are covered in Domain 6.

### **11.1.2 Cloud Data Storage Types**

Since cloud storage is virtualized it tends to support different data storage types than used in traditional storage technologies. Below the virtualization layer these might use well-known data storage mechanisms, but the cloud storage virtualization technologies that cloud users access will be different. These are the most common:

*Object storage:* Object storage is similar to a file system. “Objects” are typically files, which are then stored using a cloud-platform specific mechanism. Most access is through APIs, not standard file sharing protocols, although cloud providers may also offer front-end interfaces to support those protocols.

*Volume storage:* This is essentially a virtual hard drive for instances/virtual machines.

*Database:* Cloud platforms and providers may support a variety of different kinds of databases, including existing commercial and open source options, as well as their own proprietary systems. Proprietary databases typically use their own APIs. Commercial or open source databases are hosted by the provider and typically use existing standards for connections. These can be relational or non-relational—the latter includes NoSQL and other key/value storage systems, or file system-based databases (e.g. HDFS).

*Application/platform:* Examples of these would be a content delivery network (CDN), files stored in SaaS, caching, and other novel options.

Most cloud platforms also use redundant, durable storage mechanisms that often utilize *data dispersion* (sometimes also known as *data fragmentation of bit splitting*). This process takes chunks of data, breaks them up, and then stores multiple copies on different physical storage to provide high durability. Data stored in this way is thus physically dispersed. A single file, for example, would not be located on a single hard drive.

### **11.1.3 Managing Data Migrations to the Cloud**

Before securing the data in the cloud, most organizations want some means of managing what data is stored in private and public cloud providers. This is often essential for compliance as much or more than for security.

To start, define your policies for which data types are allowed and where they are allowed, then tie these to your baseline security requirements. For example, "Personally Identifiable Information (PII) is allowed on x services assuming it meets y encryption and access control requirements."

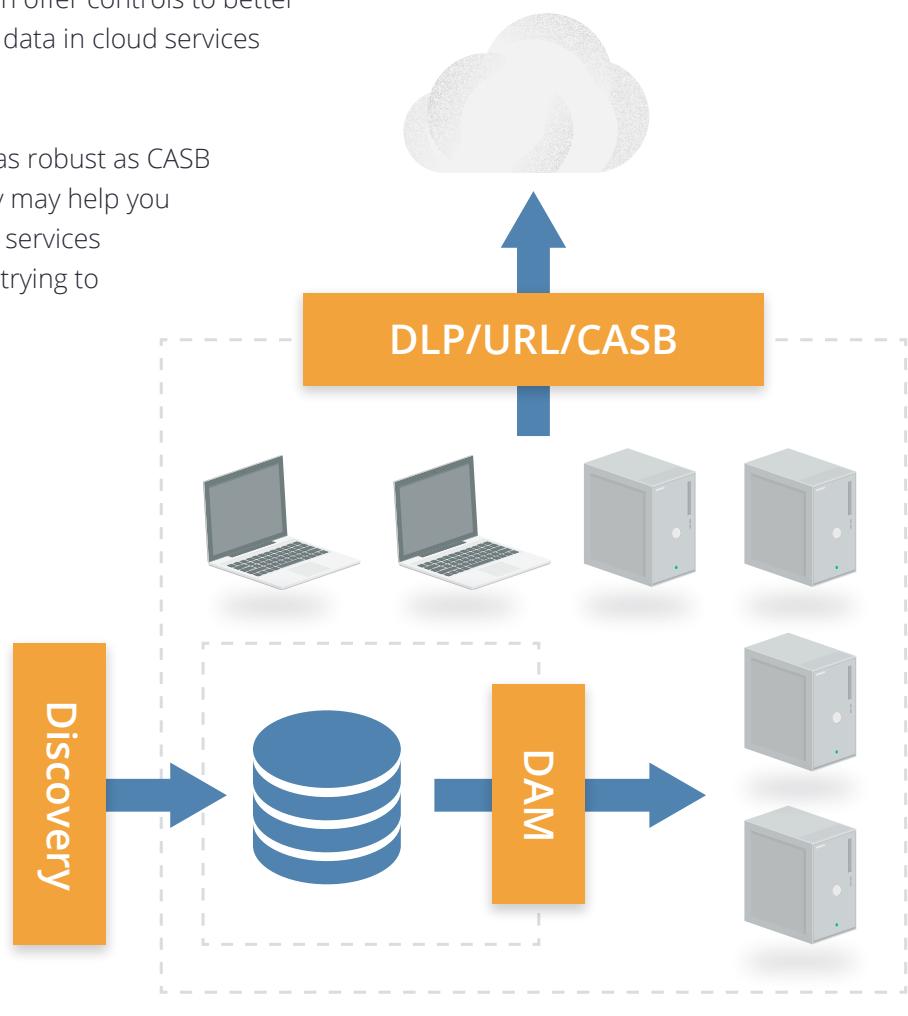
Then identify your key data repositories. Monitor them for large migrations/activity using tools such as Database Activity Monitoring and File Activity Monitoring. This is essentially building an "early warning system" for large data transfers, but it's also an important data security control to detect all sorts of major breaches and misuse scenarios.

To detect actual migrations, monitor cloud usage and any data transfers. You can do this with the help of the following tools:

**CASB:** Cloud Access and Security Brokers (also known as Cloud Security Gateways) discover internal use of cloud services using various mechanisms such as network monitoring, integrating with an existing network gateway or monitoring tool, or even by monitoring DNS queries. After discovering which services your users are connecting to, most of these products then offer monitoring of activity on approved services through API connections (when available) or inline interception (man in the middle monitoring). Many support DLP and other security alerting and even offer controls to better manage use of sensitive data in cloud services (SaaS/PaaS/and IaaS).

**URL filtering:** While not as robust as CASB a URL filter/web gateway may help you understand which cloud services your users are using (or trying to use).

**DLP:** If you monitor web traffic (and look inside SSL connections) a Data Loss Prevention (DLP) tool may also help detect data migrations to cloud services. However, some cloud SDKs and APIs may encrypt portions of data and traffic that DLP tools can't unravel, and thus they won't be able to understand the payload.



Managing data migrations to the cloud.



### 11.1.3.1 Securing Cloud Data Transfers

Ensure that you are protecting your data as it moves to the cloud. This necessitates understanding your provider's data migration mechanisms, as leveraging provider mechanisms is often more secure and cost effective than "manual" data transfer methods such as Secure File Transfer Protocol (SFTP). For example, sending data to a provider's object storage over an API is likely much more reliable and secure than setting up your own SFTP server on a virtual machine in the same provider.

There are a few options for in-transit encryption depending on what the cloud platform supports. One way is to encrypt before sending to the cloud (client-side encryption). Network encryption (TLS/SFTP/etc.) is another option. Most cloud provider APIs use Transport Layer Security (TLS) by default; if not, pick a different provider, since this is an essential security capability. Proxy-based encryption may be a third option, where you place an encryption proxy in a trusted area between the cloud user and the cloud provider and the proxy manages the encryption before transferring the data to the provider.

In some instances you may have to accept public or untrusted data. If you allow partners or the public to send you data, ensure you have security mechanisms in place to sanitize it before processing or mixing it with your existing data. Always isolate and scan this data before integrating it.

### 11.1.4 Securing Data in the Cloud

Access controls and encryption are the core data security controls across the various technologies.

#### 11.1.4.1 Cloud Data Access Controls

Access *controls* should be implemented with a minimum of three layers:

- *Management plane*: These are your controls for managing access of users that directly access the cloud platform's management plane. For example, logging in to the web console of an IaaS service will allow that user to access data in object storage. Fortunately, most cloud platforms and providers start with default deny access control policies.
- *Public and internal sharing controls*: If data is shared externally to the public or partners that don't have direct access to the cloud platform, there will be a second layer of controls for this access.
- *Application level controls*: As you build your own applications on the cloud platform you will design and implement your own controls to manage access.

Options for access controls will vary based on cloud service model and provider-specific features. Create an entitlement matrix based on platform-specific capabilities. An entitlement matrix documents which users, groups, and roles should access which resources and functions.



Entitlement	Super-Admin	Service-Admin	Storage-Admin	Dev	Security-Audit	Security-Admin
Volume Describe	X	X		X	X	X
Object Describe	X		X	X	X	X
Volume Modify	X	X		X		X
Read Logs		X			X	X

Frequently (ideally, continuously) validate that your controls meet your requirements, paying particular attention to any public shares. Consider setting up alerts for all new public shares or for changes in permissions that allow public access.

#### *Fine-Grained Access Controls and Entitlement Mappings*

The depth of potential entitlements will vary greatly from technology to technology. Some databases may support row-level security, others little more than broad access. Some will allow you to tie entitlements to identity and enforcement mechanisms built into the cloud platform, while others rely completely on the storage platform itself merely running in virtual machines.

It's important to understand your options, map them out, and build your matrix. This applies to more than just file access, of course; it also applies to databases and all your cloud data stores.

#### **11.1.4.2 Storage (At-Rest) Encryption and Tokenization**

Encryption options vary tremendously based on service model, provider, and application/deployment specifics. Key management is just as essential as encryption, and is thus covered in a subsequent section.

Encryption and tokenization are two separate technologies. Encryption protects data by applying a mathematical algorithm that "scrambles" the data, which then can only be recovered by running it through an unscrambling (decryption) process with a corresponding key. The result is a blob of ciphertext. Tokenization, on the other hand, takes the data and replaces it with a random value. It then stores the original and the randomized version in a secure database for later recovery.

Tokenization is often used when the *format* of the data is important (e.g. replacing credit card numbers in an existing system that requires the same format text string). Format Preserving Encryption encrypts data with a key but also keeps the same structural format as tokenization, but it may not be as cryptographically secure due to the compromises.

There are three components of an encryption system: data, the encryption engine, and key management. The data is, of course, the information that you're encrypting. The engine is what performs the mathematical process of encryption. Finally, the key manager handles the keys for the encryption. The overall design of the system focuses on where to put each of these components.

When designing an encryption system, you should start with a threat model. For example, do you trust a cloud provider to manage your keys? How could the keys be exposed? Where should you locate the encryption engine to manage the threats you are concerned with?

### IaaS Encryption

IaaS volumes can be encrypted using different methods, depending on your data.

#### Volume storage encryption

- *Instance-managed encryption:* The encryption engine runs within the instance, and the key is stored in the volume but protected by a passphrase or keypair.
- *Externally managed encryption:* The encryption engine runs in the instance, but the keys are managed externally and issued to the instance on request.

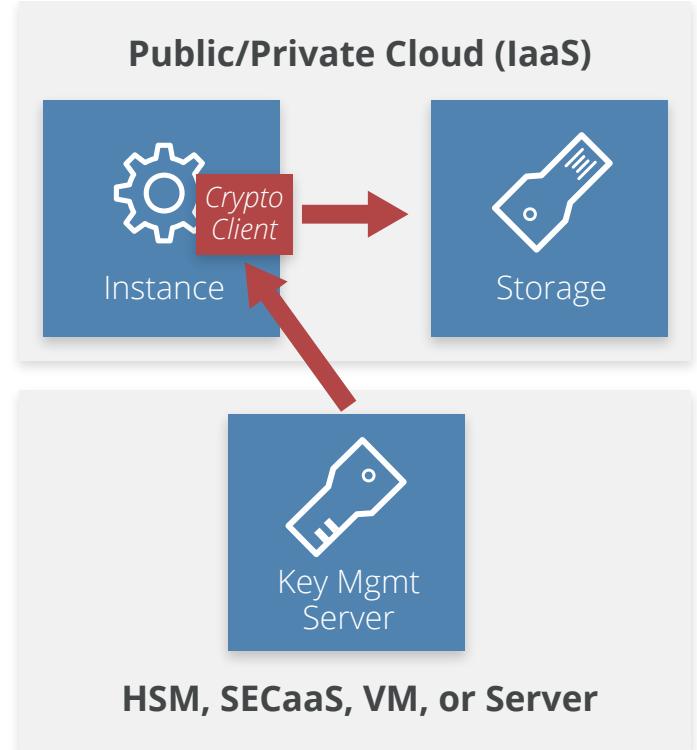
#### Object and file storage

- *Client-side encryption:* When object storage is used as the back-end for an application (including mobile applications), encrypt the data using an encryption engine embedded in the application or client.
- *Server-side encryption:* Data is encrypted on the server (cloud) side after being transferred in. The cloud provider has access to the key and runs the encryption engine.
- *Proxy encryption:* In this model, you connect the volume to a special instance or appliance/software, and then connect your instance to the encryption instance. The proxy handles all crypto operations and may keep keys either onboard or externally.

### PaaS Encryption

PaaS encryption varies tremendously due to all the different PaaS platforms.

- *Application layer encryption:* Data is encrypted in the PaaS application or the client accessing the platform.
- *Database encryption:* Data is encrypted in the database using encryption that's built in and is supported by a database platform like Transparent Database Encryption (TDE) or at the field level.
- *Other:* These are provider-managed layers in the application, such as the messaging queue. There are also IaaS options when that is used for underlying storage.



## SaaS Encryption

SaaS providers may use any of the options previously discussed. It is recommended to use per-customer keys when possible, in order to better enforce multitenancy isolation. The following options are for SaaS consumers:

- *Provider-managed encryption*: Data is encrypted in the SaaS application and generally managed by the provider.
- *Proxy encryption*: Data passes through an encryption proxy before being sent to the SaaS application.

### 11.1.4.3 Key Management (Including Customer-Managed Keys)

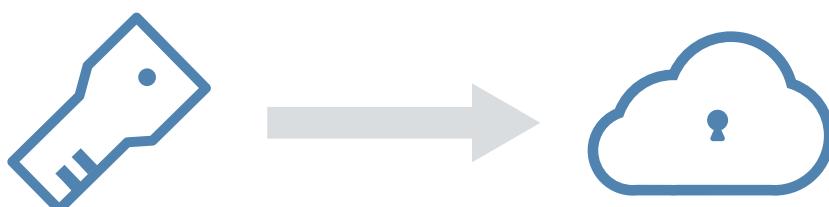
The main considerations for key management are performance, accessibility, latency, and security. Can you get the right key to the right place at the right time while also meeting your security and compliance requirements?

There are four potential options for handling key management:

- *HSM/appliance*: Use a traditional hardware security module (HSM) or appliance-based key manager, which will typically need to be on-premises, and deliver the keys to the cloud over a dedicated connection.
- *Virtual appliance/software*: Deploy a virtual appliance or software-based key manager in the cloud.
- *Cloud provider service*: This is a key management service offered by the cloud provider. Before selecting this option, make sure you understand the security model and SLAs to understand if your key could be exposed.
- *Hybrid*: You can also use a combination, such as using a HSM as the root of trust for keys but then delivering application-specific keys to a virtual appliance that's located in the cloud and only manages keys for its particular context.

### Customer-Managed Keys

A customer-managed key allows a cloud customer to manage their own encryption key while the provider manages the encryption engine. For example, using your own key to encrypt SaaS data within the SaaS platform. Many providers encrypt data by default, using keys completely in their control. Some may allow you to substitute your own key, which integrates with their encryption system. Make sure your vendor's practices align with your requirements.



*Customer managed keys.*



Some providers may require you to use a service within the provider to manage the key. Thus, although the key is customer-managed, it is still potentially available to provider. This doesn't necessarily mean it is insecure: Since the key management and data storage systems can be separated, it would require collusion on the part of multiple employees at the provider to potentially compromise data. However, keys and data could still be exposed by a government request, depending on local laws. You may be able to store the keys externally from the provider and only pass them over on a per-request basis.

### **11.1.5 Data Security Architectures**

Application architecture impacts data security. The features your cloud provider offers can reduce the attack surface, but make sure to demand strong metastructure security. For example, gap networks by using cloud storage or a queue service that communicates on the provider's network, not within your virtual network. That forces attackers to either fundamentally compromise the cloud provider or limit themselves to application-level attacks, since network attack paths are closed.

An example would be using object storage for data transfers and batch processing, rather than SFTP-ing, to static instances. Another is message queue gapping—run application components on different virtual networks that are only bridged by passing data through the cloud provider's message queue service. This eliminates network attacks from one portion of the application to the other.

### **11.1.6 Monitoring, Auditing, and Alerting**

These should tie into overall cloud monitoring. (See Domains 3, 6, and 7.) Identify (and alert about) any public access or entitlement changes on sensitive data. Use tagging to support alerting, when it's available.

You'll need to monitor both API and storage access, since data may be exposed through either—in other words, accessing data in object storage via an API call or via a public sharing URL. Activity monitoring, including Database Activity Monitoring, may be an option. Make sure to store your logs in a secure location, like a dedicated logging account.

### **11.1.7 Additional Data Security Controls**

#### **11.1.7.1 Cloud Platform/Provider-Specific Controls**

A cloud platform or provider may have data security controls that are not covered elsewhere in this domain. Although typically they will be some form of access control and encryption, this Guidance can't cover all possible options.

#### **11.1.7.2 Data Loss Prevention**

Data Loss Prevention (DLP) is typically a way to monitor and protect data that your employees access via monitoring local systems, web, email, and other traffic. It is not typically used within data centers, and thus is more applicable to SaaS than PaaS or IaaS, where it is typically not deployed.

- CASB: Some CASBs include basic DLP features for the sanctioned services they protect. For



example, you could set a policy that a credit card number is never stored in a particular cloud service. The effectiveness depends greatly on the particular tool, the cloud service, and how the CASB is integrated for monitoring. Some CASB tools can also route traffic to dedicated DLP platforms for more robust analysis than is typically available when the CASB offers DLP as a feature.

- *Cloud provider feature:* The cloud provider themselves may offer DLP capabilities, such as a cloud file storage and collaboration platform that scans uploaded files for content and applies corresponding security policies.

#### 11.1.7.3 Enterprise Rights Management

As with DLP, this is typically an employee security control that isn't always as applicable in cloud. Since all Digital Rights Management (DRM)/Enterprise Rights Management (ERM) is based on encryption, existing tools may break cloud capabilities, especially in SaaS.

- *Full DRM:* This is traditional, full digital rights management using an existing tool. For example, applying rights to a file before storing it in the cloud service. As mentioned, it may break cloud provider features, such as browser preview or collaboration, unless there is some sort of integration (which is rare at the time of this writing).
- *Provider-based control:* The cloud platform may be able to enforce controls very similar to full DRM by using native capabilities. For example, user/device/view versus edit: a policy that only allows certain users to view a file in a web browser, while other users can download and/or edit the content. Some platforms can even tie these policies to specific devices, not just on a user level.

#### 11.1.7.4 Data Masking and Test Data Generation

These are techniques to protect data used in development and test environments, or to limit real-time access to data in applications.

- *Test data generation:* This is the creation of a database with non-sensitive test data based on a "real" database. It can use scrambling and other randomization techniques to create a data set that resembles the source in size and structure but lacks sensitive data.
- *Dynamic masking:* Dynamic masking rewrites data on the fly, typically using a proxy mechanism, to mask all or part of data delivered to a user. It is usually used to protect some sensitive data in applications, for example masking out all but the last digits of a credit card number when presenting it to a user.

### 11.1.8 Enforcing Lifecycle Management Security

- *Managing data location/residency:* At certain times, you'll need to disable unneeded locations. Use encryption to enforce access at the container or object level. Then, even if the data moves to an unapproved location, the data is still protected unless the key moves with it.
- *Ensuring compliance:* You don't merely need to implement controls to maintain compliance, you need to document and test those controls. These are "artifacts of compliance;" this includes any audit artifacts you will have.
- *Backups and business continuity:* See Domain 6.

## 11.2 Recommendations

- Understand the specific capabilities of the cloud platform you are using.
- Don't dismiss cloud provider data security. In many cases it is more secure than building your own, and comes at a lower cost.
- Create an entitlement matrix for determining access controls. Enforcement will vary based on cloud provider capabilities.
- Consider CASB to monitor data flowing into SaaS. It may still be helpful for some PaaS and IaaS, but rely more on existing policies and data repository security for those types of large migrations.
- Use the appropriate encryption option based on the threat model for your data, business, and technical requirements.
- Consider use of provider-managed encryption and storage options. Where possible, use a customer-managed key.
- Leverage architecture to improve data security. Don't rely completely on access controls and encryption.
- Ensure both API and data-level monitoring are in place, and that logs meet compliance and lifecycle policy requirements
- Standards exist to help establish good security and the proper use of encryption and key management techniques and processes. Specifically, NIST SP-800-57 and ANSI X9.69 and X9.73.



# DOMAIN 12

# Identity, Entitlement, and Access Management



## 12.0 Introduction

Identity, entitlement, and access management (IAM) are deeply impacted by cloud computing. In both public and private cloud, two parties are required to manage IAM without compromising security. This domain focuses on what needs to change in identity management for cloud. While we review some fundamental concepts, the focus is on how cloud changes identity management, and what to do about it.

Cloud computing introduces multiple changes to how we have traditionally managed IAM for internal systems. It isn't that these are necessarily new issues, but that they are bigger issues when dealing with the cloud.

The key difference is the relationship between the cloud provider and the cloud user, even in private cloud. IAM can't be managed solely by one or the other and thus a trust relationship, designation of responsibilities, and the technical mechanics to enable them are required. More often than not this comes down to federation. This is exacerbated by the fact that most organizations have many (sometimes hundreds) of different cloud providers into which they need to extend their IAM.

Cloud also tends to change faster, be more distributed (including across legal jurisdictional boundaries), add to the complexity of the management plane, and rely more (often exclusively) on broad network communications for everything, which opens up core infrastructure administration to network attacks. Plus, there are extensive differences between providers and between the different service and deployment models.

This domain focuses primarily on IAM between an organization and cloud providers or between cloud providers and services. It does not discuss all the aspects of managing IAM within a cloud application, such as the internal IAM for an enterprise application running on IaaS. Those issues are very similar to building similar applications and services in traditional infrastructure.

## 12.0.1 How IAM is Different in the Cloud

Identity and access management is always complicated. At the heart we are mapping some form of an entity (a person, system, piece of code, etc.) to a verifiable identity associated with various attributes (which can change based on current circumstances), and then making a decision on what they can or can't do based on entitlements. Even when you control the entire chain of that process, managing it across disparate systems and technologies in a secure and verifiable manner, especially at scale, is a challenge.

In cloud computing, the fundamental problem is that multiple organizations are now managing the identity and access management to resources, which can greatly complicate the process. For example, imagine having to provision the same user on dozens—or hundreds—of different cloud services. Federation is the primary tool used to manage this problem, by building trust relationships between organizations and enforcing them through standards-based technologies.

Federation and other IAM techniques and technologies have existed since before the first computers (just ask a bank or government), and over time many organizations have built patchworks and silos of IAM as their IT has evolved. Cloud computing is a bit of a forcing function since adopting cloud very quickly pushes organizations to confront their IAM practices and update them to deal with the differences of cloud. This brings both opportunities and challenges.

At a high level, the migration to cloud is an opportunity to build new infrastructure and processes on modern architectures and standards. There have been tremendous advances in IAM over the years, yet many organizations have only been able to implement them in limited use cases due to budget and legacy infrastructure constraints. The adoption of cloud computing, be it a small project or an entire data center migration, means building new systems on new infrastructure that are generally architected using the latest IAM practices.

These shifts also bring challenges. Moving to federation at scale with multiple internal and external parties can be complex and difficult to manage due to the sheer mathematics of all the variables involved. Determining and enforcing attributes and entitlements across disparate systems and technologies bring both process and technical issues. Even fundamental architectural decisions may be hampered by the wide variation in support among cloud providers and platforms.

IAM spans essentially every domain in this document. This section starts with a quick review of some core terminology that not all readers may be familiar with, then delves into the cloud impacts firstly on identity, then on access and entitlement management.

## 12.1 Overview

IAM is a broad area of practice with its own lexicon that can be confusing for those who aren't domain specialists, especially since some terms have different meanings in different contexts (and are used in areas outside IAM). Even the term "IAM" is not universal and is often referred to as *Identity Management (IdM)*.

Gartner defines IAM as "**the security discipline that enables the right individuals to access the right resources at the right times for the right reasons.**" Before we get into the details, here are the high level terms most relevant to our discussion of IAM in cloud computing:

- *Entity*: the person or "thing" that will have an identity. It could be an individual, a system, a device, or application code.
- *Identity*: the unique expression of an entity within a given namespace. An entity can have multiple digital identities, such as a single individual having a work identity (or even multiple identities, depending on the systems), a social media identity, and a personal identity. For example, if you are a single entry in a single directory server then that is your identity.
- *Identifier*: the means by which an identity can be asserted. For digital identities this is often a cryptological token. In the real world it might be your passport.
- *Attributes*: facets of an identity. Attributes can be relatively static (like an organizational unit) or highly dynamic (IP address, device being used, if the user authenticated with MFA, location, etc.).
- *Persona*: the expression of an identity with attributes that indicates context. For example, a developer who logs into work and then connects to a cloud environment as a developer on a particular project. The identity is still the individual, and the persona is the individual in the context of that project.
- *Role*: identities can have multiple roles which indicate context. "Role" is a confusing and abused term used in many different ways. For our purposes we will think of it as similar to a persona, or as a subset of a persona. For example, a given developer on a given project may have different roles, such as "super-admin" and "dev", which are then used to make access decisions.
- *Authentication*: the process of confirming an identity. When you log in to a system you present a username (the identifier) and password (an attribute we refer to as an authentication factor). Also known as Authn.
- *Multifactor Authentication (MFA)*: use of multiple factors in authentication. Common options include one-time passwords generated by a physical or virtual device/token (OTP), out-of-band validation through an OTP sent via text message, or confirmation from a mobile device, biometrics, or plug-in tokens.
- *Access control*: restricting access to a resource. Access management is the process of managing access to the resources.
- *Authorization*: allowing an identity access to something (e.g. data or a function). Also known as Authz.
- *Entitlement*: mapping an identity (including roles, personas, and attributes) to an authorization. The entitlement is what they are allowed to do, and for documentation purposes we keep these in an entitlement matrix.
- *Federated Identity Management*: the process of asserting an identity across different systems or organizations. This is the key enabler of Single Sign On and also core to managing IAM in



cloud computing.

- *Authoritative source*: the “root” source of an identity, such as the directory server that manages employee identities.
- *Identity Provider*: the source of the identity in federation. The identity provider isn’t always the authoritative source, but can sometimes rely on the authoritative source, especially if it is a broker for the process.
- *Relying Party*: the system that relies on an identity assertion from an identity provider.

There are a few more terms that will be covered in their relevant sections below, including the major IAM standards. Also, although this domain may seem overly focused on public cloud, all the same principles apply in private cloud; the scope, however, will be lessened since the organization may have more control over the entire stack.

### **12.1.1 IAM Standards for Cloud Computing**

There are quite a few identity and access management standards out there, and many of them can be used in cloud computing. Despite the wide range of options the industry is settling on a core set that are most commonly seen in various deployments and are supported by the most providers. There are also some standards that are promising but aren’t yet as widely used. This list doesn’t reflect any particular endorsement and doesn’t include all options but is merely representative of what is most commonly supported by the widest range of providers:

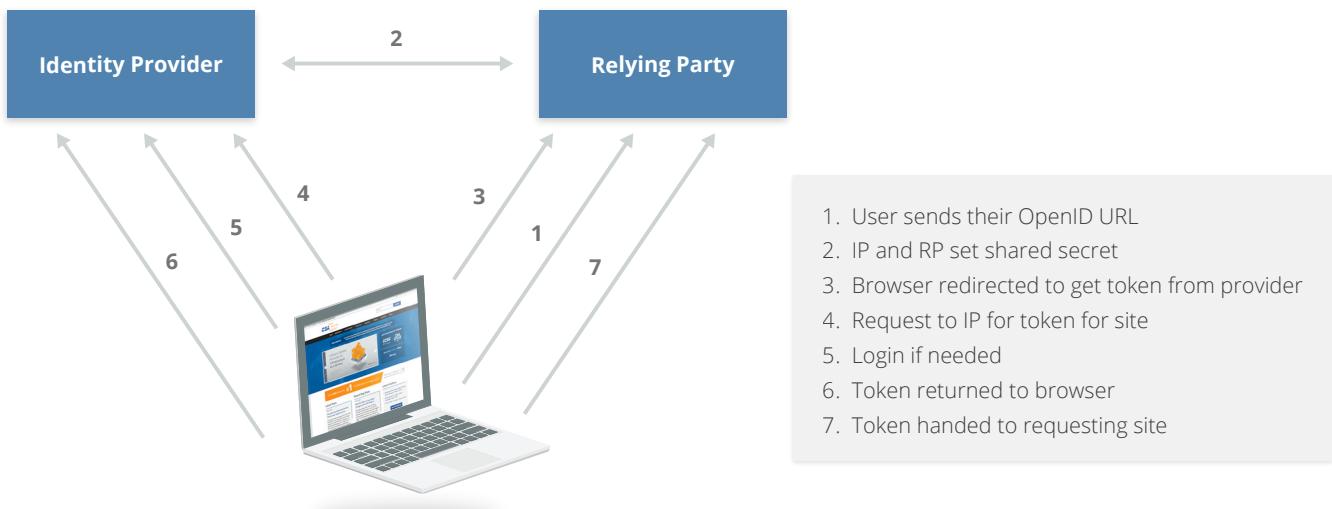
- *Security Assertion Markup Language (SAML)* 2.0 is an OASIS standard for federated identity management that supports both authentication and authorization. It uses XML to make assertions between an identity provider and a relying party. Assertions can contain authentication statements, attribute statements, and authorization decision statements. SAML is very widely supported by both enterprise tools and cloud providers but can be complex to initially configure.
- *OAuth* is an IETF standard for authorization that is very widely used for web services (including consumer services). OAuth is designed to work over HTTP and is currently on version 2.0, which is not compatible with version 1.0. To add a little confusion to the mix, OAuth 2.0 is more of a framework and less rigid than OAuth 1.0, which means implementations may not be compatible. It is most often used for delegating access control/authorizations between services.
- *OpenID* is a standard for federated authentication that is very widely supported for web services. It is based on HTTP with URLs used to identify the identity provider and the user/identity (e.g. identity.identityprovider.com). The current version is OpenID Connect 1.0 and it is very commonly seen in consumer services.

There are two other standards that aren’t as commonly encountered but can be useful for cloud computing:

- *eXtensible Access Control Markup Language (XACML)* is a standard for defining attribute-based access controls/authorizations. It is a policy language for defining access controls at a Policy Decision Point and then passing them to a Policy Enforcement Point. It can be used with both SAML and OAuth since it solves a different part of the problem—i.e. deciding what an entity is

allowed to do with a set of attributes, as opposed to handling logins or delegation of authority.

- *System for Cross-domain Identity Management (SCIM)* is a standard for exchanging identity information between domains. It can be used for provisioning and deprovisioning accounts in external systems and for exchanging attribute information.



How Federated Identity Management Works: Federation involves an *identity provider* making assertions to a *relying party* after building a trust relationship. At the heart are a series of cryptographic operations to build the trust relationship and exchange credentials. A practical example is a user logging in to their work network, which hosts a directory server for accounts. That user then opens a browser connection to a SaaS application. Instead of logging in, there are a series of behind-the-scenes operations, where the identity provider (the internal directory server) asserts the identity of the user, and that the user authenticated, as well as any attributes. The relying party trusts those assertions and logs the user in without the user entering any credentials. In fact, the relying party doesn't even have a username or password for that user; it relies on the identity provider to assert successful authentication. To the user they simply go to the website for the SaaS application and are logged in, assuming they successfully authenticated with the internal directory.

This isn't to imply there aren't other techniques or standards used in cloud computing for identity, authentication, and authorization. Most cloud providers, especially IaaS, have their own internal IAM systems that might not use any of these standards or that can be connected to an organization using these standards. For example, HTTP request signing is very commonly used for authenticating REST APIs and authorization decisions are managed by internal policies on the cloud provider side. The request signing might still support SSO through SAML, or the API might be completely OAuth based, or use its own token mechanism. All are commonly encountered, but most enterprise-class cloud providers offer federation support of some sort.

Identity protocols and standards do not represent a complete solution by themselves, but they are a means to an end.

The essential concepts when choosing an identity protocol are:

- No protocol is a silver bullet that solves all identity and access control problems.
- Identity protocols must be analyzed in the context of use case(s). For example, Browser-based Single Sign On, API keys, or mobile-to-cloud authentication could each lead companies to a different approach.
- The key operating assumption should be that identity is a perimeter in and of itself, just like a DMZ. So any identity protocol has to be selected and engineered from the standpoint that it can traverse risky territory and withstand malice.

### **12.1.2 Managing Users and Identities for Cloud Computing**

The “identity” part of identity management focuses on the processes and technologies for registering, provisioning, propagating, managing, and deprovisioning identities. Managing identities and provisioning them in systems are problems that information security has been tackling for decades. It wasn’t so long ago that IT administrators needed to individually provision users in every different internal system. Even today, with centralized directory servers and a range of standards, true Single Sign On for everything is relatively rare; users still manage a set of credentials, albeit a much smaller set than in the past.

A note on scope: The descriptions in this section are generic but do skew towards user management. The same principles apply to identities for services, devices, servers, code, and other entities, but the processes and details around those can be more complex and are tightly tied to application security and architectures. This domain also only includes limited discussion of all the internal identity management issues for cloud providers, for the same reasons. It isn’t that these areas are less important; in many cases they are more important, but they also bring a complexity that can’t be fully covered within the constraints of this Guidance.

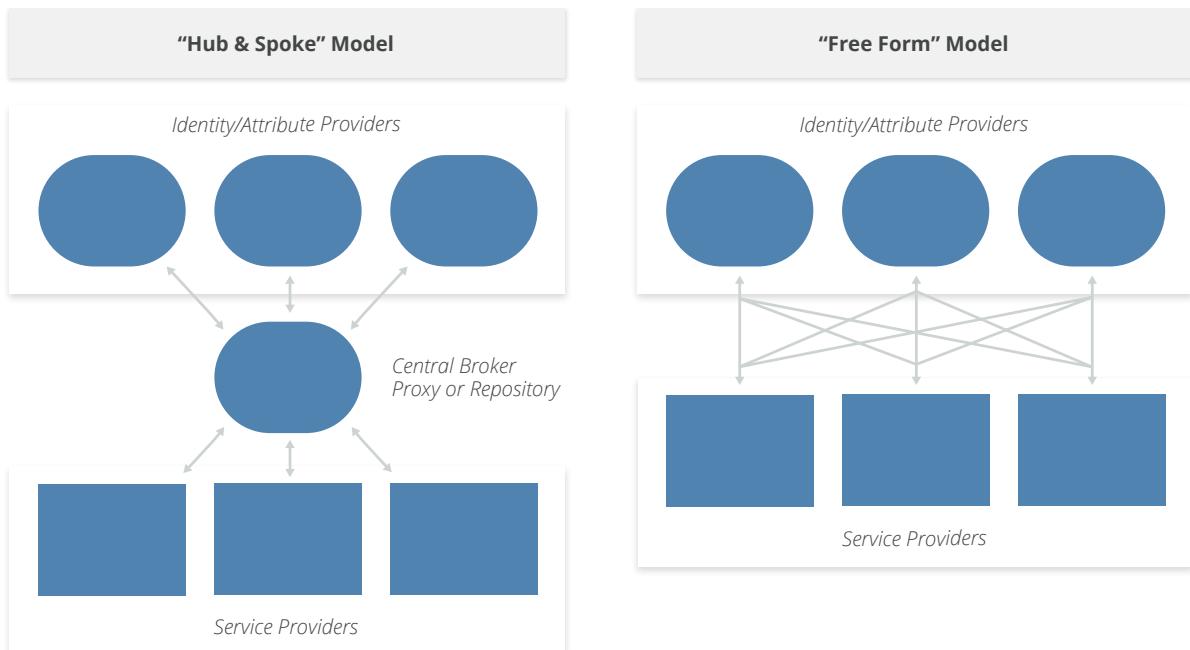
Cloud providers and cloud users need to start with the fundamental decision on how to manage identities:

- Cloud providers need to nearly always support internal identities, identifiers, and attributes for users who directly access the service, while also supporting federation so that organizations don’t have to manually provision and manage every user in the provider’s system and issue everyone separate credentials.
- Cloud users need to decide where they want to manage their identities and which architectural models and technologies they want to support to integrate with cloud providers.

As a cloud user, you can log in to a cloud provider and create all your identities in their system. This is not scalable for most organizations, which is why most turn to federation. Keep in mind there can be exceptions where it makes sense to keep all or some of the identities with the cloud provider isolated, such as backup administrator accounts to help debug problems with the federated identity connection.

When using federation, the cloud user needs to determine the authoritative source that holds the unique identities they will federate. This is often an internal directory server. The next decision is whether to directly use the authoritative source as the identity provider, use a different identity source that feeds

from the authoritative source (like a directory fed from an HR system), or to integrate an *identity broker*. There are two possible architectures:



### Free-form vs. hub and spoke

- *Free-form*: internal identity providers/sources (often directory servers) connect directly to cloud providers.
- *Hub and spoke*: internal identity providers/sources communicate with a central broker or repository that then serves as the identity provider for federation to cloud providers.

Directly federating internal directory servers in the free-form model raises a few issues:

- The directory needs Internet access. This can be a problem, depending on existing topography, or it may violate security policies.
- It may require users to VPN back to the corporate network before accessing cloud services.
- Depending on the existing directory server, and especially if you have multiple directory servers in different organizational silos, federating to an external provider may be complex and technically difficult.

*Identity brokers* handle federating between identity providers and relying parties (which may not always be a cloud service). They can be located on the network edge or even in the cloud in order to enable web-SSO.

Identity providers don't need to be located only on-premises; many cloud providers now support cloud-based directory servers that support federation internally and with other cloud services. For example, more complex architectures can synchronize or federate a portion of an organization's identities for an internal directory through an identity broker and then to a cloud-hosted directory, which then serves as an identity provider for other federated connections.



After determining the large-scale model, there are still process and architectural decisions required for any implementation:

- How to manage identities for application code, systems, devices, and other services. You may leverage the same model and standards or decide to take a different approach within cloud deployments and applications. For example, the descriptions above skew towards users accessing services, but may not apply equally for services talking to services, systems or devices, or for application components within an IaaS deployment.
- Defining the identity provisioning process and how to integrate that into cloud deployments. There may also be multiple provisioning processes for different use cases, although the goal should be to have as unified a process as possible.
  - If the organization has an effective provisioning process in place for traditional infrastructure this should ideally be extended into cloud deployments. However, if existing internal processes are problematic then the organization should instead use the move to cloud as an opportunity to build a new, more effective process.
- Provisioning and supporting individual cloud providers and deployments. There should be a formal process for adding new providers into the IAM infrastructure. This includes the process of establishing any needed federation connections, as well as:
  - Mapping attributes (including roles) between the identity provider and the relying party.
  - Enabling required monitoring/logging, including identity-related security monitoring, such as behavioral analytics.
  - Building an entitlement matrix (discussed more in the next section).
  - Documenting any break/fix scenarios in case there is a technical failure of any of the federation (or other techniques) used for the relationship.
  - Ensuring incident response plans for potential account takeovers are in place, including takeovers of privileged accounts.
- Implementing deprovisioning or entitlement change processes for identities and the cloud provider. With federation this requires work on both sides of the connection.

Lastly, cloud providers need to determine which identity management standards they wish to support. Some providers support only federation while others support multiple IAM standards plus their own internal user/account management. Providers who serve enterprise markets will need to support federated identity, and most likely SAML.

### **12.1.3 Authentication and Credentials**

Authentication is the process of proving or confirming an identity. In information security authentication most commonly refers to the act of a user logging in, but it also refers to essentially any time an entity proves who they are and assumes an identity. Authentication is the responsibility of the identity provider.

The biggest impact of cloud computing on authentication is a greater need for *strong authentication* using *multiple factors*. This is for two reasons:

- Broad network access means cloud services are always accessed over the network, and often



over the Internet. Loss of credentials could more easily lead to an account takeover by an attacker, since attacks aren't restricted to the local network.

- Greater use of federation for Single Sign On means one set of credentials can potentially compromise a greater number of cloud services.

Multifactor authentication (MFA) offers one of the strongest options for reducing account takeovers. It isn't a panacea, but relying on a single factor (password) for cloud services is very high risk. When using MFA with federation, the identity provider can and should pass the MFA status as an attribute to the relying party.

There are multiple options for MFA, including:

- *Hard tokens* are physical devices that generate one time passwords for human entry or need to be plugged into a reader. These are the best option when the highest level of security is required.
- *Soft tokens* work similarly to hard tokens but are software applications that run on a phone or computer. Soft tokens are also an excellent option but could be compromised if the user's device is compromised, and this risk needs to be considered in any threat model.
- *Out-of-band Passwords* are text or other messages sent to a user's phone (usually) and are then entered like any other one time password generated by a token. Although also a good option, any threat model must consider message interception, especially with SMS.
- *Biometrics* are growing as an option, thanks to biometric readers now commonly available on mobile phones. For cloud services, the biometric is a local protection that doesn't send biometric information to the cloud provider and is instead an attribute that can be sent to the provider. As such the security and ownership of the local device needs to be considered.

For customers, **FIDO** is one standard that may streamline stronger authentication for consumers while minimizing friction.

#### **12.1.4 Entitlement and Access Management**

The terms *entitlement*, *authorization*, and *access control* all overlap somewhat and are defined differently depending on the context. Although we defined them earlier in this section, here is a quick review.

An *authorization* is permission to do something—access a file or network, or perform a certain function like an API call on a particular resource.

An *access control* allows or denies the expression of that authorization, so it includes aspects like assuring that the user is authenticated before allowing access.

An *entitlement* maps identities to authorizations and any required attributes (e.g. user x is allowed access to resource y when z attributes have designated values). We commonly refer to a map of these entitlements as an entitlement matrix. Entitlements are often encoded as technical policies for distribution and enforcement.

This is only one definition of these terms and you may see them used differently in other documents. We also use the term access management as the "A" portion of IAM and it refers to the entire process of defining, propagating, and enforcing authorizations.

#### Sample Entitlement Matrix

Entitlement	Super-Admin	Service-1 Admin	Service-2 Admin	Dev	Security-Audit	Security-Admin
Service 1 List	X	X		X	X	X
Service 2 List	X		X	X	X	X
Service 1 Modify Network	X	X		X		X
Service 2 Modify Security Rule	X	X				X
Read Audit Logs	X				X	X

Here's a real-world cloud example. The cloud provider has an API for launching new virtual machines. That API has a corresponding authorization to allow launching new machines, with additional authorization options for what virtual network a user can launch the VM within. The cloud administrator creates an entitlement that says that users in the developer group can launch virtual machines in only their project network and only if they authenticated with MFA. The group and the use of MFA are attributes of the user's identity. That entitlement is written as a policy that is loaded into the cloud provider's system for enforcement.

Cloud impacts entitlements, authorizations, and access management in multiple ways:

- Cloud providers and platforms, like any other technology, will have their own set of potential authorizations specific to them. Unless the provider supports XACML (rare today) the cloud user will usually need to configure entitlements within the cloud platform directly.
- The cloud provider is responsible for enforcing authorizations and access controls.
- The cloud user is responsible for defining entitlements and properly configuring them within the cloud platform.
- Cloud platforms tend to have greater support for the *Attribute-Based Access Control* (ABAC) model for IAM, which offers greater flexibility and security than the *Role-Based Access Control* (RBAC) model. RBAC is the traditional model for enforcing authorizations and relies on what is often a single attribute (a defined role). ABAC allows more granular and context aware decisions by incorporating multiple attributes, such as role, location, authentication method, and more.
  - ABAC is the preferred model for cloud-based access management.
- When using federation, the cloud user is responsible for mapping attributes, including roles and groups, to the cloud provider and ensuring that these are properly communicated during authentication.

- Cloud providers are responsible for supporting granular attributes and authorizations to enable ABAC and effective security for cloud users.

### **12.1.5 Privileged User Management**

In terms of controlling risk, few things are more essential than privileged user management. The requirements mentioned above for strong authentication should be a strong consideration for any privileged user. In addition, account and session recording should be implemented to drive up accountability and visibility for privileged users.

In some cases, it will be beneficial for a privileged user to sign in through a separate tightly controlled system using higher levels of assurances for credential control, digital certificates, physically and logically separate access points, and/or jump hosts.

## **12.2 Recommendations**

- Organizations should develop a comprehensive and formalized plan and processes for managing identities and authorizations with cloud services.
- When connecting to external cloud providers, use federation, if possible, to extend existing identity management. Try to minimize silos of identities in cloud providers that are not tied to internal identities.
- Consider the use of identity brokers where appropriate.
- Cloud users are responsible for maintaining the identity provider and defining identities and attributes.
  - These should be based on an authoritative source.
  - Distributed organizations should consider using cloud-hosted directory servers when on-premises options either aren't available or do not meet requirements.
- Cloud users should prefer MFA for all external cloud accounts and send MFA status as an attribute when using federated authentication.
- Privileged identities should always use MFA.
- Develop an entitlement matrix for each cloud provider and project, with an emphasis on access to the metastructure and/or management plane.
- Translate entitlement matrices into technical policies when supported by the cloud provider or platform.
- Prefer ABAC over RBAC for cloud computing.
- Cloud providers should offer both internal identities and federation using open standards.
- There are no magic protocols: Pick your use cases and constraints first and find the right protocol second.



# DOMAIN 13

# Security as a Service



## 13.0 Introduction

While most of this Guidance focuses on securing cloud platforms and deployments, this domain shifts direction to cover security services delivered *from* the cloud. These services, which are typically SaaS or PaaS, aren't necessarily used exclusively to protect cloud deployments; they are just as likely to help defend traditional on-premises infrastructure.

Security as a Service (SecaaS) providers offer security capabilities as a cloud service. This includes dedicated SecaaS providers, as well as packaged security features from general cloud-computing providers. Security as a Service encompasses a very wide range of possible technologies, but they must meet the following criteria:

- SecaaS includes security products or services that are delivered as a cloud service.
- To be considered SecaaS, the services must still meet the essential NIST characteristics for cloud computing, as defined in Domain 1.

This section highlights some of the more common categories in the market, but SecaaS is constantly evolving and the descriptions and following list should not be considered canonical. There are examples and services not covered in this document, and more enter the market on a constant basis.

# 13.1 Overview

## 13.1.1 Potential Benefits and Concerns of SecaaS

Before delving into the details of the different significant SecaaS categories it is important to understand how SecaaS is different from both on-premises and self-managed security. To do so, consider the potential benefits and consequences.

### 13.1.1.1 Potential Benefits

- *Cloud-computing benefits.* The normal potential benefits of cloud computing—such as reduced capital expenses, agility, redundancy, high availability, and resiliency—all apply to SecaaS. As with any other cloud provider the magnitude of these benefits depend on the pricing, execution, and capabilities of the security provider.
- *Staffing and expertise.* Many organizations struggle to employ, train, and retain security professionals across relevant domains of expertise. This can be exacerbated due to limitations of local markets, high costs for specialists, and balancing day-to-day needs with the high rate of attacker innovation. As such, SecaaS providers bring the benefit of extensive domain knowledge and research that may be unattainable for many organizations that are not solely focused on security or the specific security domain.
- *Intelligence-sharing.* SecaaS providers protect multiple clients simultaneously and have the opportunity to share data intelligence and data across them. For example, finding a malware sample in one client allows the provider to immediately add it to their defensive platform, thus protecting all other customers. Practically speaking this isn't a magic wand, as the effectiveness will vary across categories, but since intelligence-sharing is built into the service, the potential upside is there.
- *Deployment flexibility.* SecaaS may be better positioned to support evolving workplaces and cloud migrations, since it is itself a cloud-native model delivered using broad network access and elasticity. Services can typically handle more flexible deployment models, such as supporting distributed locations without the complexity of multi-site hardware installations.
- *Insulation of clients.* In some cases, SecaaS can intercept attacks before they hit the organization directly. For example, spam filtering and cloud-based Web Application Firewalls are positioned *between* the attackers and the organization. They can absorb certain attacks before they ever reach the customer's assets.
- *Scaling and cost.* The cloud model provides the consumer with a "Pay as You Grow" model, which also helps organizations focus on their core business and lets them leave security concerns to the experts.

### 13.1.1.2 Potential Concerns

- *Lack of visibility.* Since services operate at a remove from the customer, they often provide less visibility or data compared to running one's own operation. The SecaaS provider may not reveal details of how it implements its own security and manages its own environment. Depending on the service and the provider, that may result in a difference in data sources and the level of detail available for things like monitoring and incidents. Some information that the customer



may be accustomed to having may look different, have gaps, or not be available at all. The actual evidence and artifacts of compliance, as well as other investigative data, may not meet the customer's goals. All of this can and should be determined before entering into any agreement.

- *Regulation differences.* Given global regulatory requirements, SecaaS providers may be unable to assure compliance in all jurisdictions that an organization operates in.
- *Handling of regulated data.* Customers will also need assurance that any regulated data potentially vacuumed up as part of routine security scanning or a security incident is handled in accordance with any compliance requirements; this also needs to comply with aforementioned international jurisdictional differences. For example, employee monitoring in Europe is more restrictive than it is in the United States, and even basic security monitoring practices could violate workers' rights in that region. Likewise, if a SecaaS provider relocates its operations, due to data center migration or load balancing, it may violate regulations that have geographical restrictions in data residence.
- *Data leakage.* As with any cloud computing service or product, there is always the concern of data from one cloud user leaking to another. This risk isn't unique to SecaaS, but the highly sensitive nature of security data (and other regulated data potentially exposed in security scanning or incidents) does mean that SecaaS providers should be held to the highest standards of multitenant isolation and segregation. Security-related data is also likely to be involved in litigation, law enforcement investigations, and other discovery situations. Customers want to ensure their data will not be exposed when these situations involve another client on the service.
- *Changing providers.* Although simply switching SecaaS providers may on the surface seem easier than swapping out on-premises hardware and software, organizations may be concerned about lock-in due to potentially losing access to data, including historical data needed for compliance or investigative support.
- *Migration to SecaaS.* For organizations that have existing security operations and on-premises legacy security control solutions, the migration to SecaaS and the boundary and interface between any in-house IT department and SecaaS providers must be well planned, exercised, and maintained.

### **13.1.2 Major Categories of Security as a Service Offerings**

There are a large number of products and services that fall under the heading of Security as a Service. While the following is not a canonical list, it describes many of the more common categories seen as of this writing.

#### **13.1.2.1 Identity, Entitlement, and Access Management Services**

Identity-as-a-service is a generic term that covers one or many of the services that may comprise an identity ecosystem, such as Policy Enforcement Points (PEP-as-a-service), Policy Decision Points (PDP-as-a-service), Policy Access Points (PAP-as-a-service), services that provide Entities with Identity, services that provide attributes (e.g. Multi-Factor Authentication), and services that provide reputation.

One of the better-known categories heavily used in cloud security is Federated Identity Brokers. These services help intermediate IAM between an organization's existing identity providers (internal



or cloud-hosted directories) and the many different cloud services used by the organization. They can provide web-based Single Sign On (SSO), helping ease some of the complexity of connecting to a wide range of external services that use different federation configurations.

There are two other categories commonly seen in cloud deployments. Strong authentication services use apps and infrastructure to simplify the integration of various strong authentication options, including mobile device apps and tokens for MFA. The other category hosts directory servers in the cloud to serve as an organization's identity provider.

#### **13.1.2.2 Cloud Access and Security Brokers (CASB, also known as Cloud Security Gateways)**

These products intercept communications that are directed towards a cloud service or directly connect to the service via API in order to monitor activity, enforce policy, and detect and/or prevent security issues. They are most commonly used to manage an organization's sanctioned and unsanctioned SaaS services. While there are on-premises CASB options, it is also often offered as a cloud-hosted service.

CASBs can also connect to on-premises tools to help an organization detect, assess, and potentially block cloud usage and unapproved services. Many of these tools include risk-rating capabilities to help customers understand and categorize hundreds or thousands of cloud services. The ratings are based on a combination of the provider's assessments, which can be weighted and combined with the organization's priorities.

Most providers also offer basic Data Loss Prevention for the covered cloud services, inherently or through partnership and integration with other services.

Depending on the organization discussing "CASB," the term is also sometimes used to include Federated Identity Brokers. This can be confusing: Although the combination of the "security gateway" and "identity broker" capabilities is possible and does exist, the market is still dominated by independent services for those two capabilities.

#### **13.1.2.3 Web Security (Web Security Gateways)**

Web Security involves real-time protection, offered either on-premises through software and/or appliance installation, or via the Cloud by proxying or redirecting web traffic to the cloud provider (or a hybrid of both). This provides an added layer of protection on top of other protection, such as anti-malware software to prevent malware from entering the enterprise via activities such as web browsing. In addition, it can also enforce policy rules around types of web access and the time frames when they are allowed. Application authorization management can provide an extra level of granular and contextual security enforcement for web applications.

#### **13.1.2.4 Email Security**

Email Security should provide control over inbound and outbound email, protecting the organization from risks like phishing and malicious attachments, as well as enforcing corporate policies like acceptable use and spam prevention, and providing business continuity options.



In addition, the solution may support policy-based encryption of emails as well as integrating with various email server solutions. Many email security solutions also offer features like digital signatures that enable identification and non-repudiation. This category includes the full range of services, from those as simple as anti-spam features all the way to fully-integrated email security gateways with advanced malware and phishing protection.

### 13.1.2.5 Security Assessment

Security assessments are third-party or customer-driven audits of cloud services or assessments of on-premises systems via cloud-provided solutions. Traditional security assessments for infrastructure, applications, and compliance audits are well defined and supported by multiple standards such as NIST, ISO, and CIS. A relatively mature toolset exists, and a number of tools have been implemented using the SecaaS delivery model. Using that model, subscribers get the typical benefits of cloud computing: variant elasticity, negligible setup time, low administration overhead, and pay-per-use with low initial investments.

There are three main categories of security assessments:

- Traditional security/vulnerability assessments of assets that are deployed in the cloud (e.g. virtual machines/instances for patches and vulnerabilities) or on-premises.
- Application security assessments, including SAST, DAST, and management of RASP.
- Cloud platform assessment tools that connect directly with the cloud service over API to assess not merely the assets deployed in the cloud, but the cloud configuration as well.

### 13.1.2.6 Web Application Firewalls

In a cloud-based WAF, customers redirect traffic (using DNS) to a service that analyzes and filters traffic before passing it through to the destination web application. Many cloud WAFs also include anti-DDoS capabilities.

### 13.1.2.7 Intrusion Detection/Prevention (IDS/IPS)

Intrusion Detection/Prevention systems monitor behavior patterns using rule-based, heuristic, or behavioral models to detect anomalies in activity which might present risks to the enterprise. With IDS/IPS as a service, the information feeds into a service-provider's managed platform, as opposed to the customer being responsible for analyzing events themselves. Cloud IDS/IPS can use existing hardware for on-premises security, virtual appliances for in-cloud (see Domain 7 for the limitations), or host-based agents.

### 13.1.2.8 Security Information & Event Management (SIEM)

Security Information and Event Management systems aggregate (via push or pull mechanisms) log and event data from virtual and real networks, applications, and systems. This information is then correlated and analyzed to provide real-time reporting on and alerting of information or events that may require intervention or other types of responses. Cloud SIEMs collect this data in a cloud service, as opposed to a customer-managed, on-premises system.



### 13.1.2.9 Encryption and Key Management

These services encrypt data and/or manage encryption keys. They may be offered by cloud services to support customer-managed encryption and data security. They may be limited to only protecting assets within that specific cloud provider, or they may be accessible across multiple providers (and even on-premises, via API) for broader encryption management. The category also includes encryption proxies for SaaS, which intercept SaaS traffic to encrypt discrete data.

However, encrypting data *outside* a SaaS platform may affect the ability of the platform to utilize the data in question.

### 13.1.2.10 Business Continuity and Disaster Recovery

Providers of cloud BC/DR services back up data from individual systems, data centers, or cloud services to a cloud platform instead of relying on local storage or shipping tapes. They may use a local gateway to speed up data transfers and local recoveries, with the cloud service serving as the final repository for worst-case scenarios or archival purposes.

### 13.1.2.11 Security Management

These services roll up traditional security management capabilities, such as EPP (endpoint) protection, agent management, network security, mobile device management, and so on into a single cloud service. This reduces or eliminates the need for local management servers and may be particularly well suited for distributed organizations.

### 13.1.2.12 Distributed Denial of Service Protection

By nature, most DDoS protections are cloud-based. They operate by rerouting traffic through the DDoS service in order to absorb attacks before they can affect the customer's own infrastructure.

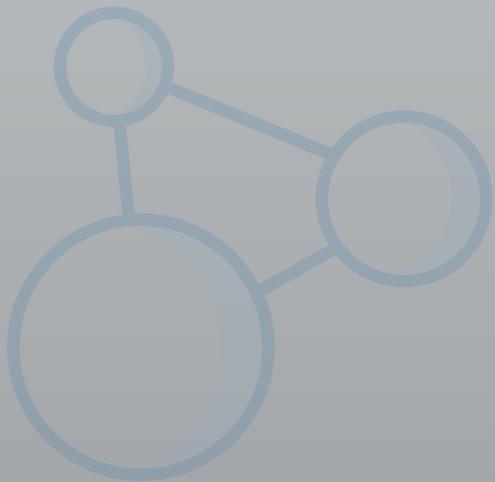
## 13.2 Recommendations

- Before engaging a SecaaS provider, be sure to understand any security-specific requirements for data-handling (and availability), investigative, and compliance support.
- Pay particular attention to handling of regulated data, like PII.
- Understand your data retention needs and select a provider that can support data feeds that don't create a lock-in situation.
- Ensure that the SecaaS service is compatible with your current and future plans, such as its supported cloud (and on-premises) platforms, the workstation and mobile operating systems it accommodates, and so on.



# DOMAIN 14

## Related Technologies



### 14.0 Introduction

Throughout this Guidance we have focused on providing background information and best practices for directly securing cloud computing. As such a foundational technology, there are also a variety of related technologies that bring their own particular security concerns.

While covering all potential uses of cloud is well beyond the scope of this document, CSA feels it is important to include background and recommendations for key technologies that are interrelated with cloud. Some, such as containers and Software-Defined Networks, are so tightly intertwined that we cover them in other respective domains of the Guidance. This Domain provides more depth on additional technologies that don't fit cleanly into existing domains.

Breaking these out into their own section provides more flexibility to update coverage, adding and removing technologies as their usage shifts and new capabilities emerge.

### 14.1 Overview

Related technologies fall into two broad categories:

- Technologies that rely nearly exclusively on cloud computing to operate.
- Technologies that don't necessarily rely on cloud, but are commonly seen in cloud deployments.

That isn't to say these technologies *can't* work without cloud, just that they are often seen overlapping or relying on cloud deployments and are so commonly seen that they have implications for the majority of cloud security professionals.

The current list includes:

- Big Data

- Internet of Things (IoT)
- Mobile devices
- Serverless computing

Each of these technologies is currently covered by additional Cloud Security Alliance research working groups in multiple ongoing projects and publications:

- [Big Data Working Group](#)
- [Internet of Things Working Group](#)
- [Mobile Working Group](#)

### 14.1.1 Big Data

Big data includes a collection of technologies for working with extremely large datasets that traditional data-processing tools are unable to manage. It's not any single technology but rather refers commonly to distributed collection, storage, and data-processing frameworks.

Gartner defines it as such: "**Big data is high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization.**"

The "3 Vs" are commonly accepted as the core definition of big data, although there are many other interpretations.

- *High volume*: a large size of data, in terms of number of records or attributes.
- *High velocity*: fast generation and processing of data, i.e., real-time or stream data.
- *High variety*: structured, semi-structured, or unstructured data.

Cloud computing, due to its elasticity and massive storage capabilities, is very often where big data projects are deployed. Big data is not exclusive to cloud by any means, but big data technologies are very commonly integrated into cloud-computing applications and offered by cloud providers as IaaS or PaaS.

There are three common components of big data, regardless of the specific toolset used:

- *Distributed data collection*: Mechanisms to ingest large volumes of data, often of a streaming nature. This could be as "lightweight" as web-click streaming analytics and as complex as highly distributed scientific imaging or sensor data. Not all big data relies on distributed or streaming data collection, but it is a core big data technology.
- *Distributed storage*: The ability to store the large data sets in distributed file systems (such as Google File System, Hadoop Distributed File System, etc.) or databases (often NoSQL), which is often required due to the limitations of non-distributed storage technologies.
- *Distributed processing*: Tools capable of distributing processing jobs (such as map reduce, spark, etc.) for the effective analysis of data sets so massive and rapidly changing that single-origin processing can't effectively handle them.



#### **14.1.1.1 Security and Privacy Considerations**

Due to a combination of the highly distributed nature of big data applications (with data collection, storage, and processing all distributed among diverse nodes) and the sheer volume and potential sensitivity of the information, security and privacy are typically high priorities but are challenged by a patchwork of different tools and platforms.

#### **14.1.1.2 Data Collection**

Data collection mechanisms will likely use intermediary storage that needs to be appropriately secured. This storage is used as part of the transfer of data from collection to storage. Even if primary storage is well-secured it's important to also check intermediary storage, which might be as simple as some swap space on a processing node. For example, if collection is run in containers or virtual machines, ensure the underlying storage is appropriately secured. Distributed analysis/processing nodes will also likely use some form of intermediate storage that will need additional security. This could be, for example, the volume storage for instances running processing jobs.

#### **14.1.1.3 Key Management**

Key management for storage may be complicated depending on the exact mechanisms used due to the distributed nature of nodes. There are techniques to properly encrypt most big data storage layers today, and these align with our guidance in *Domain 11- Data Security and Encryption*. The complicating factor is that key management needs to handle distributing keys to multiple storage and analysis nodes.

#### **14.1.1.4 Security Capabilities**

Not all big data technologies have robust security capabilities. In some cases cloud provider security capabilities can help compensate for the big data technology limitations. Both should be included in any security architecture and the details will be specific to the combination of technologies selected.

#### **14.1.1.5 Identity and Access Management**

Identity and Access Management will likely occur at both cloud and big data tool levels, which can complicate entitlement matrices.

#### **14.1.1.6 PaaS**

Many cloud providers are expanding big data support with *machine learning* and other platform as a service options that rely on access to enterprise data. These should not be used without a full understanding of potential data exposure, compliance, and privacy implications. For example, if the machine learning runs as PaaS inside the provider's infrastructure, where provider employees could technically access it, does that create a compliance exposure?

This doesn't mean you shouldn't use the services, it just means you need to understand the implications and make appropriate risk decisions. Machine learning and other analysis services aren't necessarily insecure and don't necessarily violate privacy and compliance commitments.

## **14.1.2 Internet of Things (IoT)**

The Internet of Things is a blanket term for non-traditional computing devices used in the physical world that utilize Internet connectivity. It includes everything from Internet-enabled operational technology (used by utilities like power and water) to fitness trackers, connected lightbulbs, medical devices, and beyond. These technologies are increasingly deployed in enterprise environments for applications such as:

- Digital tracking of the supply chain.
- Digital tracking of physical logistics.
- Marketing, retail, and customer relationship management.
- Connected healthcare and lifestyle applications for employees, or delivered to consumers.

A very large percentage of these devices connect back to cloud computing infrastructure for their back-end processing and data storage. Key cloud security issues related to IoT include:

- Secure data collection and sanitization.
- Device registration, authentication, and authorization. One common issue encountered today is use of stored credentials to make direct API calls to the back-end cloud provider. There are known cases of attackers decompiling applications or device software and then using those credentials for malicious purposes.
- API security for connections from devices back to the cloud infrastructure. Aside from the stored credentials issue just mentioned, the APIs themselves could be decoded and used for attacks on the cloud infrastructure.
- Encrypted communications. Many current devices use weak, outdated, or non-existent encryption, which places data and the devices at risk.
- Ability to patch and update devices so they don't become a point of compromise. Currently, it is common for devices to be shipped as-is and never receive security updates for operating systems or applications. This has already caused multiple significant and highly publicized security incidents, such as massive botnet attacks based on compromised IoT devices.

## **14.1.3 Mobile**

Mobile computing is neither new nor exclusive to cloud, but a very large percentage of mobile applications connect to cloud computing for their back-end processing. Cloud can be an ideal platform to support mobile since cloud providers are geographically distributed and designed for the kinds of highly dynamic workloads commonly experienced with mobile applications. This section won't discuss overall mobile security, just the portions that affect cloud security.

The primary security issues for mobile computing (in the cloud context) are very similar to IoT, except a mobile phone or tablet is also a general purpose computer:

- Device registration, authentication, and authorization are common sources of issues. Especially (again), the use of stored credentials, and even more so when the mobile device



connects directly to the cloud provider's infrastructure/APIs. Attackers have been known to decompile mobile applications to reveal stored credentials which are then used to directly manipulate or attack the cloud infrastructure. Data stored on the device should also be protected with the assumption that the user of the device may be a hostile attacker.

- Application APIs are also a potential source of compromise. Attackers are known to sniff API connections, in some cases using local proxies that they redirect their own devices towards, and then decompile the (likely now unencrypted) API calls and explore them for security weaknesses. Certificate pinning/validation inside the device application may help reduce this risk.

For additional recommendations on the security of mobile and cloud computing see the latest research from the CSA [Mobile Working Group](#).

#### **14.1.4 Serverless Computing**

Serverless computing is the extensive use of certain PaaS capabilities to such a degree that all or some of an application stack runs in a cloud provider's environment without any customer-managed operating systems, or even containers.

"Serverless computing" is a bit of a misnomer since there is always a server running the workload someplace, but those servers and their configuration and security are completely hidden from the cloud user. The consumer only manages settings for the service, and not any of the underlying hardware and software stacks.

Serverless includes services such as:

- Object storage
- Cloud load balancers
- Cloud databases
- Machine learning
- Message queues
- Notification services
- Code execution environments (These are generally restricted containers where a consumer runs uploaded application code.)
- API gateways
- Web servers

Serverless capabilities may be deeply integrated by the cloud provider and tied together with event-driven systems and integrated IAM and messaging to support construction of complex applications without any customer management of servers, containers, or other infrastructure.

From a security standpoint, key issues include:

- Serverless places a much higher security burden on the cloud provider. Choosing your provider and understanding security SLAs and capabilities is absolutely critical.
- Using serverless, the cloud user will not have access to commonly-used monitoring and



logging levels, such as server or network logs. Applications will need to integrate more logging, and cloud providers should provide necessary logging to meet core security and compliance requirements.

- Although the provider's services may be certified or attested for various compliance requirements, not necessarily every service will match every potential regulation. Providers need to keep compliance mappings up to date, and customers need to ensure they only use services within their compliance scope.
- There will be high levels of access to the cloud provider's management plane since that is the only way to integrate and use the serverless capabilities.
- Serverless can dramatically reduce attack surface and pathways and integrating serverless components may be an excellent way to break links in an attack chain, even if the entire application stack is not serverless.
- Any vulnerability assessment or other security testing must comply with the provider's terms of service. Cloud users may no longer have the ability to directly test applications, or must test with a reduced scope, since the provider's infrastructure is now hosting everything and can't distinguish between legitimate tests and attacks.
- Incident response may also be complicated and will definitely require changes in process and tooling to manage a serverless-based incident.

## 14.2 Recommendations

- Big data
  - Leverage cloud provider capabilities wherever possible, even if they overlap with big data tool security capabilities. This ensures you have proper protection within the cloud metastructure and the specific application stack.
  - Use encryption for primary, intermediary, and backup storage for both data collection and data storage planes.
  - Include both the big data tool and cloud platform Identity and Access Management in the project entitlement matrix.
  - Fully understand the potential benefits and risks of using a cloud machine-learning or analytics service. Pay particular attention to privacy and compliance implications.
    - Cloud providers should ensure customer data is not exposed to employees or other administrators using technical and process controls.
    - Cloud providers should clearly publish which compliance standards their analytics and machine-learning services are compliant with (for their customers).
    - Cloud users should consider use of data masking or obfuscation when considering a service that doesn't meet security, privacy, or compliance requirements.
  - Follow additional big data security best practices, including those provided by the tool vendor (or Open Source project) and the [Cloud Security Alliance](#).
- Internet of Things
  - Ensure devices can be patched and upgraded.
  - Do not store static credentials on devices that could lead to compromise of the cloud application or infrastructure.
  - Follow best practices for secure device registration and authentication to the cloud-side



- Cloud icon
- Warning icon
- Search icon
- Database icon
- Network icon
- File transfer icon
- Grid icon
- Cloud icon
- Shield icon
- Laptop icon
- Cloud icon
- Cloud icon
- Network icon

application, typically using a federated identity standard.

- Encrypt communications.
- Use a secure data collection pipeline and sanitize data to prevent exploitation of the cloud application or infrastructure through attacks on the data-collection pipeline.
- Assume all API requests are hostile.
- Follow the additional, more-detailed guidance issued by the CSA [Internet of Things Working Group](#).

- Mobile

- Follow your cloud provider's guidance on properly authenticating and authorizing mobile devices when designing an application that connects directly to the cloud infrastructure.
- Use industry standards, typically federated identity, for connecting mobile device applications to cloud-hosted applications.
- Never transfer unencrypted keys or credentials over the Internet.
- Test all APIs under the assumption that a hostile attacker will have authenticated, unencrypted access.
  - Consider certificate pinning and validation inside mobile applications.
  - Validate all API data and sanitize for security.
  - Implement server/cloud-side security monitoring for hostile API activity.
- Ensure all data stored on device is secured and encrypted.
  - Sensitive data that could allow compromise of the application stack should not be stored locally on-device where a hostile user can potentially access it.
- Follow the more detailed recommendations and research issued by the [CSA Mobile Working Group](#).

- Serverless Computing

- Cloud providers must clearly state which PaaS services have been assessed against which compliance requirements or standards.
- Cloud users must only use serverless services that match their compliance and governance obligations.
- Consider injecting serverless components into application stacks using architectures that reduce or eliminate attack surface and/or network attack paths.
- Understand the impacts of serverless on security assessments and monitoring.
  - Cloud users will need to rely more on application-code scanning and logging and less on server and network logs.
- Cloud users must update incident response processes for serverless deployments.
- Although the cloud provider is responsible for security below the serverless platform level, the cloud user is still responsible for properly configuring and using the products.

Information Assurance Framework



## ABOUT ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard for information on good practices. Moreover, the agency facilitates contacts between European institutions, the Member States, and private business and industry actors.

## CONTACT DETAILS:

This report has been edited by:

e-mail: [Daniele.catteddu@enisa.europa.eu](mailto:Daniele.catteddu@enisa.europa.eu) and [Giles.hogben@enisa.europa.eu](mailto:Giles.hogben@enisa.europa.eu),

Internet: <http://www.enisa.europa.eu/>

### Legal notice

Notice must be taken that this publication represents the views and interpretations of the editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent the state-of-the-art in cloud computing and it may be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2009

**INFORMATION ASSURANCE FRAMEWORK****CONTENTS**

About ENISA.....	2
Contact details:.....	2
Target Audience.....	5
Methodology .....	5
1. Information Assurance Framework.....	6
2. Managing risk .....	7
3. Division of liabilities .....	7
4. Division of responsibilities.....	8
4.1. Software as a Service.....	8
4.2. Platform as a Service .....	9
4.3. Infrastructure as a Service.....	9
4.3.1. Application Security in Infrastructure as a service .....	10
5. Note of caution .....	11
5.1. Note to governments .....	11
6. Information assurance requirements .....	12
6.1. Personnel security .....	12
6.2. Supply-chain assurance .....	12
6.3. Operational security .....	13
6.3.1. Software assurance .....	14
6.3.2. Patch management.....	14

6.3.3.	Network architecture controls.....	14
6.3.4.	Host architecture .....	15
6.3.5.	PaaS – Application security .....	15
6.3.6.	SaaS – Application security .....	15
6.3.7.	Resource provisioning.....	16
6.4.	Identity and access management .....	16
6.4.1.	Authorisation .....	16
6.4.2.	Identity provisioning .....	17
6.4.3.	Management of personal data .....	17
6.4.4.	Key management .....	17
6.4.5.	Encryption .....	17
6.4.6.	Authentication .....	18
6.4.7.	Credential compromise or theft .....	18
6.4.8.	Identity and access management systems offered to the cloud customer.....	18
6.5.	Asset management .....	19
6.6.	Data and Services Portability .....	19
6.7.	Business Continuity Management .....	20
6.7.1.	Incident management and response .....	20
6.8.	Physical security.....	22
6.9.	Environmental controls.....	23
6.10.	Legal requirements .....	24

## INFORMATION ASSURANCE FRAMEWORK

## TARGET AUDIENCE

The intended audience of this report are:

- Business leaders, in particular SME's to evaluate and mitigate the risks of adopting cloud computing technologies.
- Cloud Provider to standardize their cloud computing service compliance process vis a vis laws and regulations
- European policymakers to decide on research policy (to develop technologies to mitigate risks).
- European policymakers to decide on appropriate policy and economic incentives, legislative measures, awareness-raising initiatives etc vis-a-vis cloud-computing technologies.

## METHODOLOGY

The key sections of this document are based on the broad classes of controls from the ISO 27001/2 and BS25999 standards. Details within these sections are derived from both the standard, as well as industry best practice requirements. Throughout, we have selected only those controls which are relevant to cloud providers and third party outsourcers.

The detailed framework scheduled for release in 2010 is intended to include additional standards such as NIST SP 800-53.

## 1. INFORMATION ASSURANCE FRAMEWORK

One of the most important recommendations in the ENISA's Cloud Computing Risk Assessment report (see [full version](#)) is the Information Assurance Framework, a set of assurance criteria designed to:

1. assess the risk of adopting cloud services (comparing the risks of maintaining a 'classical' organization and architecture with risks to migrate in a cloud computing environment) and
2. compare different Cloud Provider offers
3. obtain assurance from the selected cloud providers. The preparation of effective security questionnaires for third party service providers is a significant resource drain for cloud customers and one which is difficult to achieve without expertise in cloud-specific architectures.
4. reduce the assurance burden on cloud providers. A very important risk specific to cloud infrastructures is introduced by the requirement for NIS assurance. Many cloud providers find that a large number of customers request audits of their infrastructure and policies. This can create a critically high burden on security personnel and it also increases the number of people with access to the infrastructure, which significantly increases the risk of attack due to misuse of security-critical information, theft of critical or sensitive data etc. Cloud providers will need to deal with this by establishing clear framework for handling such requests.

The Framework provides a set of questions that an organisation can ask a cloud provider to assure themselves that they are sufficiently protecting the information entrusted to them.

These questions are intended to provide a minimum baseline any organisation may therefore have additional specific requirements not covered within the baseline.

Equally this document does not provide a standard response format for the cloud provider, so responses are in a free text format. However it is intended to feed into a more detailed comprehensive framework which will be developed as a follow-up to this work, allowing a consistent, comparable set of responses. Such responses will provide a quantifiable metric as to the Information Assurance maturity of the provider.

It is intended for the aforementioned metric to be consistent against other providers that allow a comparison for end user organisations.

**INFORMATION ASSURANCE FRAMEWORK**

## 2. MANAGING RISK

It is worth noting that although it is possible to transfer many of the risks to an externally provisioned supplier, the true cost of transferring risk is very rarely realised. For example, a security incident that results in the unauthorised disclosure of customer data may result in financial loss to the provider, however the negative publicity and loss of consumer confidence, and potential regulatory penalties (PCI-DSS) would be felt by the end customer. Such a scenario highlights the importance of distinguishing risk, with commercial risk. In that it is possible to transfer commercial risk, but the true risk always remains with the end customer.

Any response to the results of a risk assessment - in particular the amount and type of investment in mitigation, should be decided on the basis of the risk appetite of the organisation and the opportunities and financial savings which are lost by following any particular risk mitigation strategy.

Cloud customers should also carry out their own, context-specific risk analysis. Some of available Risk Management / Risks Assessment methodologies can be found at: [http://rm-inv.enisa.europa.eu/rm\\_ra\\_methods.html](http://rm-inv.enisa.europa.eu/rm_ra_methods.html)

As the business and regulatory environment changes and new risks arise, risk assessment should be a regular activity rather than a one off event.

## 3. DIVISION OF LIABILITIES

The following table shows the expected division of liabilities between customer and provider.

	<b>Customer</b>	<b>Provider</b>
<b>Lawfulness of content</b>	Full liability	Intermediary liability with Liability exemptions under the terms of the E-commerce Directive and its interpretation. <sup>1</sup>

<sup>1</sup> Cf. definition of information society services as provided for in Art. 2 of Directive 98/48/EC as well as Art. 2 of Directive 2000/31/EC, in conjunction with exemptions contained in Articles 12-15 of Directive 2000/31/EC (e-Commerce Directive).

<b>Security incidents</b> (including data leakage, use of account to launch an attack)	Responsibility for due diligence for what is under its control according to contractual conditions	Responsibility for due diligence for what is under its control
<b>European Data Protection Law status</b>	Data controller	Data processor (external)

## 4. DIVISION OF RESPONSIBILITIES

With respect to security incidents, there needs to be a clear definition and understanding between the customer and the provider of security-relevant roles and responsibilities. The lines of such a division will vary greatly between SaaS offerings and IaaS offerings, with the latter delegating more responsibility to the customer. A typical and rational division of responsibility is shown in the following table. *In any case, for each type of service, the customer and provider should clearly define which of them is responsible for all the items on the list below.* In the case of standard terms of service (ie, no negotiation possible), cloud customers should verify what lies within their responsibility.

### 4.1. SOFTWARE AS A SERVICE

Customer	Provider
<ul style="list-style-type: none"> <li>• Compliance with data protection law in respect of customer data collected and processed</li> <li>• Maintenance of identity management system</li> <li>• Management of identity management system</li> <li>• Management of authentication platform (including enforcing password policy)</li> </ul>	<ul style="list-style-type: none"> <li>• Physical support infrastructure (facilities, rack space, power, cooling, cabling, etc)</li> <li>• Physical infrastructure security and availability (servers, storage, network bandwidth, etc)</li> <li>• OS patch management and hardening procedures (check also any conflict between customer hardening procedure and provider security policy)</li> <li>• Security platform configuration (Firewall rules, IDS/IPS tuning, etc)</li> <li>• Systems monitoring</li> <li>• Security platform maintenance (Firewall, Host IDS/IPS, antivirus, packet filtering)</li> <li>• Log collection and security monitoring</li> </ul>

## INFORMATION ASSURANCE FRAMEWORK

## 4.2. PLATFORM AS A SERVICE

Customer	Provider
<ul style="list-style-type: none"> <li>• Maintenance of identity management system</li> <li>• Management of identity management system</li> <li>• Management of authentication platform (including enforcing password policy)</li> </ul>	<ul style="list-style-type: none"> <li>• Physical support infrastructure (facilities, rack space, power, cooling, cabling, etc)</li> <li>• Physical infrastructure security and availability (servers, storage, network bandwidth, etc)</li> <li>• OS patch management and hardening procedures (check also any conflict between customer hardening procedure and provider security policy)</li> <li>• Security platform configuration (firewall rules, IDS/IPS tuning, etc)</li> <li>• Systems monitoring</li> <li>• Security platform maintenance (firewall, Host IDS/IPS, antivirus, packet filtering)</li> <li>• Log collection and security monitoring</li> </ul>

## 4.3. INFRASTRUCTURE AS A SERVICE

Customer	Provider
<ul style="list-style-type: none"> <li>• Maintenance of identity management system</li> <li>• Management of identity management system</li> <li>• Management of authentication platform (including enforcing password policy)</li> <li>• Management of guest OS patch and hardening procedures (check also any conflict between customer hardening procedure and provider security policy)</li> <li>• Configuration of guest security platform (firewall rules, IDS/IPS tuning, etc)</li> </ul>	<ul style="list-style-type: none"> <li>• Physical support infrastructure (facilities, rack space, power, cooling, cabling, etc)</li> <li>• Physical infrastructure security and availability (servers, storage, network bandwidth, etc)</li> <li>• Host Systems (hypervisor, virtual firewall, etc)</li> </ul>

- |   |  |
|---|--|
| <ul style="list-style-type: none"><li>• Guest systems monitoring</li><li>• Security platform maintenance (firewall, Host IDS/IPS, antivirus, packet filtering)</li><li>• Log collection and security monitoring</li></ul> |  |
|---|--|

Where cloud customers are responsible for the security of their Infrastructures (in IaaS), they should consider the following:

#### 4.3.1. APPLICATION SECURITY IN INFRASTRUCTURE AS A SERVICE

IaaS application providers treat the applications within the customer virtual instance as a ‘black box’ and therefore are completely agnostic to the operations and management of a customer’s applications. The entire ‘stack’ – customer application, run time application platform (.Net, Java, Ruby, PHP etc) is run on the customers’ server (on provider infrastructure) and is managed by customers themselves. For this reason it is vitally important to note that the customer must take full responsibility for securing their cloud deployed applications. Here is a brief checklist/description relating to best practice for secure application design and management:

- Cloud deployed applications must be designed for the internet threat model (even if they are deployed as part of VPC - virtual private cloud).
- They must be designed/embedded with standard security countermeasures to guard against the common web vulnerabilities (see OWASP guides ).
- Customers are responsible for keeping their applications up to date – and must therefore ensure they have a patch strategy (to ensure their applications are screened from malware and hackers scanning for vulnerabilities to gain unauthorised access to their data within the cloud)
- Customers should not be tempted to use custom implementations of Authentication, Authorisation and Accounting (AAA) as these can become weak if not properly implemented.

In summary – enterprise distributed cloud applications must run with many controls in place to secure host (and network – see previous section), user access, application level controls (see OWASP guides relating to secure web/online application design). Also please note many main stream vendors such as Microsoft, Oracle, Sun etc publish comprehensive documentation on how to secure the configuration of their products.

**INFORMATION ASSURANCE FRAMEWORK**

## 5. NOTE OF CAUTION

The series of questions detailed within the proceeding section are a selection of common controls. It is not intended to be an exhaustive list; equally certain questions may not be applicable to particular implementations. Subsequently this list should be used as a baseline of common controls, and further detail should be sought where required.

### 5.1. NOTE TO GOVERNMENTS

The following controls are aimed primarily at SMEs assessing cloud providers. They may also be useful to governments with the following provisos. *The characteristics of the cloud used should be considered carefully in relation to any government body's information classification scheme.*

- The use of public clouds – even with favourable responses from the following questionnaire – is not recommended for anything but the lowest assurance classes of data.
- For higher assurance classes of data, the list of suggested checks in this report is valid but should be supplemented with additional checks. This report is not intended to cover such controls, but the following are examples of issues which should be covered:
  - Does the provider offer transparent information and full control over the current physical location of all data? High assurance data is often restricted by location.
  - Does the provider support the data classification scheme used?
  - What guarantees does the provider offer that customer resources are fully isolated (e.g., no sharing of physical machines)?
  - Assuming physical machines are not shared between customers, to what degree are storage, memory and other data traces fully erased before machines are reallocated.
  - Does the provider support or even mandate physical token based 2-factor authentication for client access?
  - Does the provider hold ISO 27001/2 certification? What is the scope of the certification?
  - Do the products used by the provider have Common Criteria certifications? At which level? Which protection profile and security target for the product?

## 6. INFORMATION ASSURANCE REQUIREMENTS

### 6.1. PERSONNEL SECURITY

The majority of questions relating to personnel will be similar to those you would ask your own IT personnel or other personnel who are dealing with your IT. As with most assessments, there is a balance between the risks and the cost.

- What policies and procedures do you have in place when hiring your IT administrators or others with system access? These should include:
  - pre-employment checks (identity, nationality or status, employment history and references, criminal convictions, and vetting (for senior personnel in high privilege roles)).
- Are there different policies depending on where the data is stored or applications are run?
  - For example, hiring policies in one region may be different from those in another.
  - Practices need to be consistent across regions.
  - It may be that sensitive data is stored in one particular region with appropriate personnel.
- What security education program do you run for all staff?
- Is there a process of continuous evaluation?
  - How often does this occur?
  - Further interviews
  - Security access and privilege reviews
  - Policy and procedure reviews.

### 6.2. SUPPLY-CHAIN ASSURANCE

The following questions apply where the cloud provider subcontracts some operations that are key to the security of the operation to third parties (eg, a SaaS provider outsourcing the underlying platform to a third party provider, a cloud provider outsourcing the security services to a managed security services provider, use of an external provider for identity management of operating systems, etc). It also includes third parties with physical or remote access to the cloud provider infrastructure. It is assumed that this entire questionnaire may be applied recursively to third (or nth) party cloud service providers.

- Define those services that are outsourced or subcontracted in your service delivery supply chain that are key to the security (including availability) of your operations.
- Detail the procedures used to assure third parties accessing your infrastructure (physical and/or logical).
  - Do you audit your outsourcers and subcontractors and how often?
- Are any SLA provisions guaranteed by outsourcers lower than the SLAs you offer to your customers? If not, do you have supplier redundancy in place?

**INFORMATION ASSURANCE FRAMEWORK**

- What measures are taken to ensure third party service levels are met and maintained?
- Can the cloud provider confirm that security policy and controls are applied (contractually) to their third party providers?

### 6.3. OPERATIONAL SECURITY

It is expected that any commercial agreement with external providers will include service levels for all network services. However, in addition to the defined agreements, the end customer should still ensure that the provider employs appropriate controls to mitigate unauthorised disclosure.

- Detail your change control procedure and policy. This should also include the process used to re-assess risks as a result of changes and clarify whether the outputs are available to end customers.
- Define the remote access policy.
- Does the provider maintain documented operating procedures for information systems?
- Is there a staged environment to reduce risk, e.g., development, test and operational environments, and are they separated?
- Define the host and network controls employed to protect the systems hosting the applications and information for the end customer. These should include details of certification against external standards (e.g., ISO 27001/2).
- Specify the controls used to protect against malicious code.
- Are secure configurations deployed to only allow the execution of authorised mobile code and authorised functionality (e.g., only execute specific commands)?
- Detail policies and procedures for backup. This should include procedures for the management of removable media and methods for securely destroying media no longer required. (Depending on his business requirements, the customer may wish to put in place an independent backup strategy. This is particularly relevant where time-critical access to back-up is required.)

Audit logs are used in the event of an incident requiring investigation; they can also be used for troubleshooting. For these purposes, the end customer will need assurance that such information is available:

- Can the provider detail what information is recorded within audit logs?
  - For what period is this data retained?
  - Is it possible to segment data within audit logs so they can be made available to the end customer and/or law enforcement without compromising other customers and still be admissible in court?
  - What controls are employed to protect logs from unauthorised access or tampering?
  - What method is used to check and protect the integrity of audit logs?

- How are audit logs reviewed? What recorded events result in action being taken?
- What time source is used to synchronise systems and provide accurate audit log time stamping?

#### 6.3.1. SOFTWARE ASSURANCE

- Define controls used to protect the integrity of the operating system and applications software used. Include any standards that are followed, e.g., OWASP, SANS Checklist , SAFECode.
- How do you validate that new releases are fit-for-purpose or do not have risks (backdoors, Trojans, etc)? Are these reviewed before use?
- What practices are followed to keep the applications safe?
- Is a software release penetration tested to ensure it does not contain vulnerabilities? If vulnerabilities are discovered, what is the process for remedying these?

#### 6.3.2. PATCH MANAGEMENT

- Provide details of the patch management procedure followed.
- Can you ensure that the patch management process covers all layers of the cloud delivery technologies – i.e., network (infrastructure components, routers and switches, etc), server operating systems, virtualisation software, applications and security subsystems (firewalls, antivirus gateways, intrusion detection systems, etc)?

#### 6.3.3. NETWORK ARCHITECTURE CONTROLS

- Define the controls used to mitigate DDoS (distributed denial-of-service) attacks.
  - Defence in depth (deep packet analysis, traffic throttling, packet black-holing, etc)
  - Do you have defences against ‘internal’ (originating from the cloud providers networks) attacks as well as external (originating from the Internet or customer networks) attacks?
- What levels of isolation are used?
  - for virtual machines, physical machines, network, storage (e.g., storage area networks), management networks and management support systems, etc.
- Does the architecture support continued operation from the cloud when the company is separated from the service provider and vice versa (e.g., is there a critical dependency on the customer LDAP system)?
- Is the virtual network infrastructure used by cloud providers (in PVLANS and VLAN tagging 802.1q architecture) secured to vendor and/or best practice specific standards (e.g., are MAC spoofing, ARP poisoning attacks, etc, prevented via a specific security configuration)?

**INFORMATION ASSURANCE FRAMEWORK****6.3.4. HOST ARCHITECTURE**

- Does the provider ensure virtual images are hardened by default?
- Is the hardened virtual image protected from unauthorized access?
- Can the provider confirm that the virtualised image does not contain the authentication credentials?
- Is the host firewall run with only the minimum ports necessary to support the services within the virtual instance?
- Can a host-based intrusion prevention service (IPS) be run in the virtual instance?

**6.3.5. PaaS – APPLICATION SECURITY**

Generally speaking, PaaS service providers are responsible for the security of the platform software stack, and the recommendations throughout this document are a good foundation for ensuring a PaaS provider has considered security principles when designing and managing their PaaS platform. It is often difficult to obtain detailed information from PaaS providers on exactly how they secure their platforms – however the following questions, along with other sections within this document, should be of assistance in assessing their offerings.

- Request information on how multi-tenanted applications are isolated from each other – a high level description of containment and isolation measures is required.
- What assurance can the PaaS provider give that access to your data is restricted to your enterprise users and to the applications you own?
- The platform architecture should be classic ‘sandbox’ – does the provider ensure that the PaaS platform sandbox is monitored for new bugs and vulnerabilities?
- PaaS providers should be able to offer a set of security features (re-useable amongst their clients) – do these include user authentication, single sign on, authorisation (privilege management), and SSL/TLS (made available via an API)?

**6.3.6. SaaS – APPLICATION SECURITY**

The SaaS model dictates that the provider manages the entire suite of applications delivered to end-users. Therefore SaaS providers are mainly responsible for securing these applications. Customers are normally responsible for operational security processes (user and access management). However the following questions, along with other sections within this document, should assist in assessing their offerings:

- What administration controls are provided and can these be used to assign read and write privileges to other users?

- Is the SaaS access control fine grained and can it be customised to your organisations policy?

#### 6.3.7. RESOURCE PROVISIONING

- In the event of resource overload (processing, memory, storage, network)?
  - What information is given about the relative priority assigned to my request in the event of a failure in provisioning?
  - Is there a lead time on service levels and changes in requirements?
- How much can you scale up? Does the provider offer guarantees on maximum available resources within a minimum period?
- How fast can you scale up? Does the provider offer guarantees on the availability of supplementary resources within a minimum period?
- What processes are in place for handling large-scale trends in resource usage (eg, seasonal effects)?

### 6.4. IDENTITY AND ACCESS MANAGEMENT

The following controls apply to the cloud provider's identity and access management systems (those under their control).

#### 6.4.1. AUTHORISATION

- Do any accounts have system-wide privileges for the entire cloud system and, if so, for what operations (read/write/delete)?
- How are the accounts with the highest level of privilege authenticated and managed?
- How are the most critical decisions (e.g., simultaneous de-provisioning of large resource blocks) authorised (single or dual, and by which roles within the organisation)?
- Are any high-privilege roles allocated to the same person? Does this allocation break the segregation of duties or least privilege rules?
- Do you use role-based access control (RBAC)? Is the principle of least privilege followed?
- What changes, if any, are made to administrator privileges and roles to allow for extraordinary access in the event of an emergency?
- Is there an 'administrator' role for the customer? For example, does the customer administrator have a role in adding new users (but without allowing him to change the underlying storage!)?

**INFORMATION ASSURANCE FRAMEWORK****6.4.2. IDENTITY PROVISIONING**

- What checks are made on the identity of user accounts at registration? Are any standards followed? For example, the e-Government Interoperability Framework?
  - Are there different levels of identity checks based on the resources required?
- What processes are in place for de-provisioning credentials?
- Are credentials provisioned and de-provisioned simultaneously throughout the cloud system, or are there any risks in de-provisioning them across multiple geographically distributed locations?

**6.4.3. MANAGEMENT OF PERSONAL DATA**

- What data storage and protection controls apply to the user directory (eg, AD, LDAP) and access to it?
- Is user directory data exportable in an interoperable format?
- Is need-to-know the basis for access to customer data within the cloud provider?

**6.4.4. KEY MANAGEMENT**

For keys under the control of the cloud provider:

- Are security controls in place for reading and writing those keys? For example, strong password policies, keys stored in a separate system, hardware security modules (HSM) for root certificate keys, smart card based authentication, direct shielded access to storage, short key lifetime, etc.
- Are security controls in place for using those keys to sign and encrypt data?
- Are procedures in place in the event of a key compromise? For example, key revocation lists.
- Is key revocation able to deal with simultaneity issues for multiple sites?
- Are customer system images protected or encrypted?

**6.4.5. ENCRYPTION**

- Encryption can be used in multiple places – where is it used?
  - data in transit
  - data at rest
  - data in processor or memory?
- Usernames and passwords?
- Is there a well-defined policy for what should be encrypted and what should not be encrypted?

- Who holds the access keys?
- How are the keys protected?

#### 6.4.6. AUTHENTICATION

- What forms of authentication are used for operations requiring high assurance? This may include login to management interfaces, key creation, access to multiple-user accounts, firewall configuration, remote access, etc.
  - Is two-factor authentication used to manage critical components within the infrastructure, such as firewalls, etc?

#### 6.4.7. CREDENTIAL COMPROMISE OR THEFT

- Do you provide anomaly detection (the ability to spot unusual and potentially malicious IP traffic and user or support team behaviour)? For example, analysis of failed and successful logins, unusual time of day, and multiple logins, etc.
- What provisions exist in the event of the theft of a customer's credentials (detection, revocation, evidence for actions)?

#### 6.4.8. IDENTITY AND ACCESS MANAGEMENT SYSTEMS OFFERED TO THE CLOUD CUSTOMER

The following questions apply to the identity and access management systems which are offered by the cloud provider for use and control by the cloud customer.

##### 6.4.8.1. IDENTITY MANAGEMENT FRAMEWORKS

- Does the system allow for a federated IDM infrastructure which is interoperable both for high assurance (OTP systems, where required) and low assurance (eg. username and password)?
- Is the cloud provider interoperable with third party identity providers?
- Is there the ability to incorporate single sign-on?

##### 6.4.8.2. ACCESS CONTROL

- Does the client credential system allow for the separation of roles and responsibilities and for multiple domains (or a single key for multiple domains, roles and responsibilities)?
- How do you manage access to customer system images – and ensure that the authentication and cryptographic keys are not contained within them?

**INFORMATION ASSURANCE FRAMEWORK****6.4.8.3. AUTHENTICATION**

- How does the cloud provider identify itself to the customer (ie, is there mutual authentication)?
  - when the customer sends API commands?
  - when the customer logs into the management interface?
- Do you support a federated mechanism for authentication?

**6.5. ASSET MANAGEMENT**

It is important to ensure the provider maintains a current list of hardware and software (applications) assets under the cloud providers control. This enables checks that all systems have appropriate controls employed, and that systems cannot be used as a backdoor into the infrastructure.

- Does the provider have an automated means to inventory all assets, which facilitates their appropriate management?
- Is there a list of assets that the customer has used over a specific period of time?

The following questions are to be used where the end customer is deploying data that would require additional protection (i.e.. deemed as sensitive).

- Are assets classified in terms of sensitivity and criticality?
  - If so, does the provider employ appropriate segregation between systems with different classifications and for a single customer who has systems with different security classifications?

**6.6. DATA AND SERVICES PORTABILITY**

This set of questions should be considered in order to understand the risks related to vendor lock-in.

- Are there documented procedures and APIs for exporting data from the cloud?
- Does the vendor provide interoperable export formats for all data stored within the cloud?
- In the case of SaaS, are the API interfaces used standardised?
- Are there any provisions for exporting user-created applications in a standard format?
- Are there processes for testing that data can be exported to another cloud provider – should the client wish to change provider, for example?
- Can the client perform their own data extraction to verify that the format is universal and is capable of being migrated to another cloud provider?

## 6.7. BUSINESS CONTINUITY MANAGEMENT

Providing continuity is important to an organisation. Although it is possible to set service level agreements detailing the minimum amount of time systems are available, there remain a number of additional considerations.

- Does the provider maintain a documented method that details the impact of a disruption?
  - What are the RPO (recovery point objective) and RTO (recovery time objective) for services? Detail according to the criticality of the service.
  - Are information security activities appropriately addressed in the restoration process?
  - What are the lines of communication to end customers in the event of a disruption?
  - Are the roles and responsibilities of teams clearly identified when dealing with a disruption?
- Has the provider categorised the priority for recovery, and what would be our relative priority (the end customer) to be restored? Note: this may be a category (HIGH/MED/LOW).
- What dependencies relevant to the restoration process exist? Include suppliers and outsource partners.
- In the event of the primary site being made unavailable, what is the minimum separation for the location of the secondary site?

### 6.7.1. INCIDENT MANAGEMENT AND RESPONSE

Incident management and response is a part of business continuity management. The goal of this process is to contain the impact of unexpected and potentially disrupting events to an acceptable level for an organization.

To evaluate the capacity of an organization to minimize the probability of occurrence or reduce the negative impact of an information security incident, the following questions should be asked to a cloud provider:

- Does the provider have a formal process in place for detecting, identifying, analyzing and responding to incidents?
- Is this process rehearsed to check that incident handling processes are effective? Does the provider also ensure, during the rehearsal, that everyone within the cloud provider's support organisation is aware of the processes and of their roles during incident handling (both during the incident and post analysis)?
- How are the detection capabilities structured?
  - How can the cloud customer report anomalies and security events to the provider?
  - What facilities does the provider allow for customer-selected third party RTSM services to intervene in their systems (where appropriate) or to co-ordinate incident response capabilities with the cloud provider?

**INFORMATION ASSURANCE FRAMEWORK**

- Is there a real time security monitoring (RTSM) service in place? Is the service outsourced? What kind of parameters and services are monitored?
- Do you provide (upon request) a periodical report on security incidents (eg., according to the ITIL definition)?
- For how long are the security logs retained? Are those logs securely stored? Who has access to the logs?
- Is it possible for the customer to build a HIPS/HIDS in the virtual machine image? Is it possible to integrate the information collected by the intrusion detection and prevention systems of the customer into the RTSM service of the cloud provider or that of a third party?
- How are severity levels defined?
- How are escalation procedures defined? When (if ever) is the cloud customer involved?
- How are incidents documented and evidence collected?
- Besides authentication, accounting and audit, what other controls are in place to prevent (or minimize the impact of) malicious activities by insiders?
- Does the provider offer the customer (upon request) a forensic image of the virtual machine?
- Does the provider collect incident metrics and indicators (ie., number of detected or reported incidents per months, number of incidents caused by the cloud provider's subcontractors and the total number of such incidents, average time to respond and to resolve, etc?).
  - Which of these does the provider make publicly available (NB not all incident reporting data can be made public since it may compromise customer confidentiality and reveal security critical information)??)
- How often does the provider test disaster recovery and business continuity plans?
- Does the provider collect data on the levels of satisfaction with SLAs?
- Does the provider carry out help desk tests? For example:
  - Impersonation tests (is the person at the end of the phone requesting a password reset, really who they say they are?) or so called 'social engineering' attacks.
- Does the provider carry out penetration testing? How often? What are actually tested during the penetration test – for example, do they test the security isolation of each image to ensure it is not possible to 'break out' of one image into another and also gain access to the host infrastructure?. The tests should also check to see if it is possible to gain access, via the virtual image, to the cloud providers management and support systems (e.g, example the provisioning and admin access control systems).
- Does the provider carry out vulnerability testing? How often?
- What is the process for rectifying vulnerabilities (hot fixes, re-configuration, uplift to later versions of software, etc)?

## 6.8. PHYSICAL SECURITY

As with personnel security, many of the potential issues arise because the IT infrastructure is under the control of a third party – like traditional outsourcing, the effect of a physical security breach can have an impact on multiple customers (organizations).

- What assurance can you provide to the customer regarding the physical security of the location? Please provide examples, and any standards that are adhered to, eg., Section 9 of ISO 27001/2.
  - Who, other than authorised IT personnel, has unescorted (physical) access to IT infrastructure?
    - For example, cleaners, managers, ‘physical security’ staff, contractors, consultants, vendors, etc.
  - How often are access rights reviewed?
    - How quickly can access rights be revoked?
  - Do you assess security risks and evaluate perimeters on a regular basis?
    - How frequently?
  - Do you carry out regular risk assessments which include things such as neighboring buildings?
  - Do you control or monitor personnel (including third parties) who access secure areas?
  - What policies or procedures do you have for loading, unloading and installing equipment?
  - Are deliveries inspected for risks before installation?
  - Is there an up-to-date physical inventory of items in the data centre?
  - Do network cables run through public access areas?
    - Do you use armoured cabling or conduits?
  - Do you regularly survey premises to look for unauthorized equipment?
  - Is there any off-site equipment?
    - How is this protected?
  - Do your personnel use portable equipment (eg., laptops, smart phones) which can give access to the data centre?
    - How are these protected?
  - What measures are in place to control access cards?
  - What processes or procedures are in place to destroy old media or systems when required to do so?
    - data overwritten?
    - physical destruction?

**INFORMATION ASSURANCE FRAMEWORK**

- What authorization processes are in place for the movement of equipment from one site to another?
  - How do you identify staff (or contractors) who are authorized to do this?
- How often are equipment audits carried out to monitor for unauthorised equipment removal?
- How often are checks made to ensure that the environment complies with the appropriate legal and regulatory requirements?

## 6.9. ENVIRONMENTAL CONTROLS

- What procedures or policies are in place to ensure that environmental issues do not cause an interruption to service?
- What methods do you use to prevent damage from a fire, flood, earthquake, etc?
  - In the event of a disaster, what additional security measures are put in place to protect physical access?
  - Both at the primary as well as at the secondary sites?
- Do you monitor the temperature and humidity in the data centre?
  - Air-conditioning considerations or monitoring?
- Do you protect your buildings from lightening strikes?
  - Including electrical and communication lines?
- Do you have stand-alone generators in the event of a power failure?
  - For how long can they run?
  - Are there adequate fuel supplies?
  - Are there failover generators?
  - How often do you check UPS equipment?
  - How often do you check your generators?
  - Do you have multiple power suppliers?
- Are all utilities (electricity, water, etc) capable of supporting your environment?
  - How often is this re-evaluated and tested?
- Is your air-conditioning capable of supporting your environment?
  - How often is it tested?
- Do you follow manufacturers recommended maintenance schedules?
- Do you only allow authorised maintenance or repair staff onto the site?
  - How do you check their identity?
- When equipment is sent away for repair, is the data cleaned from it first?
  - How is this done?

## 6.10. LEGAL REQUIREMENTS

Customers and potential customers of cloud provider services should have regard to their respective national and supra-national obligations for compliance with regulatory frameworks and ensure that any such obligations are appropriately complied with.

The key legal questions the customer should ask the cloud provider are:

- In what country is the cloud provider located?
- Is the cloud provider's infrastructure located in the same country or in different countries?
- Will the cloud provider use other companies whose infrastructure is located outside that of the cloud provider?
- Where will the data be physically located?
- Will jurisdiction over the contract terms and over the data be divided?
- Will any of the cloud provider's services be subcontracted out?
- Will any of the cloud provider's services be outsourced?
- How will the data provided by the customer and the customer's customers, be collected, processed and transferred?
- What happens to the data sent to the cloud provider upon termination of the contract?



**National Institute of  
Standards and Technology**  
U.S. Department of Commerce

Special Publication 500-292

---

# **NIST Cloud Computing Reference Architecture**

---

## **Recommendations of the National Institute of Standards and Technology**

---

Fang Liu, Jin Tong, Jian Mao, Robert Bohn,  
John Messina, Lee Badger and Dawn Leaf

NIST Special Publication 500-292

NIST Cloud Computing Reference  
Architecture

*Recommendations of the National  
Institute of Standards and Technology*

Fang Liu, Jin Tong, Jian Mao, Robert  
Bohn, John Messina, Lee Badger and  
Dawn Leaf

---

## Information Technology Laboratory

---

Cloud Computing Program  
Information Technology Laboratory  
National Institute of Standards and Technology  
Gaithersburg, MD 20899-8930

September 2011



**U.S. Department of Commerce**

Rebecca M. Blank, Acting Secretary

**National Institute of Standards and Technology**

Patrick D. Gallagher, Under Secretary for Standards  
and Technology and Director

## Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

**National Institute of Standards and Technology Special Publication 500-292  
Natl. Inst. Stand. Technol. Spec. Publ. 500-292, 35 pages (September 2011)**

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

## **Acknowledgments**

The authors, Fang Liu, Jin Tong, Jian Mao of Knowcean Consulting Inc. (services acquired via US NAVY SPAWAR contract), Robert Bohn, John Messina, Lee Badger, Dawn Leaf of the National Institute of Standards and Technology (NIST), wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content. The authors gratefully acknowledge and appreciate the broad contributions from members of the NIST Cloud Computing Reference Architecture and Taxonomy Working Group and the Reference Architecture Analysis Team.

## **Trademark Information**

All names are trademarks or registered trademarks of their respective owners.

## Table of Contents

<b>Executive Summary.....</b>	<b>vi</b>
<b>1. Introduction.....</b>	<b>1</b>
<b>1.1 Background.....</b>	<b>1</b>
<b>1.2 Objectives.....</b>	<b>1</b>
<b>1.3 How This Report Was Produced.....</b>	<b>2</b>
<b>1.4 Structure of This Report.....</b>	<b>2</b>
<b>2. Cloud Computing Reference Architecture: An Overview .....</b>	<b>3</b>
<b>2.1 The Conceptual Reference Model.....</b>	<b>3</b>
<b>2.2 Cloud Consumer.....</b>	<b>5</b>
<b>2.3 Cloud Provider .....</b>	<b>7</b>
<b>2.4 Cloud Auditor .....</b>	<b>8</b>
<b>2.5 Cloud Broker.....</b>	<b>8</b>
<b>2.6 Cloud Carrier .....</b>	<b>8</b>
<b>2.7 Scope of Control between Provider and Consumer .....</b>	<b>9</b>
<b>3. Cloud Computing Reference Architecture: Architectural Components .....</b>	<b>10</b>
<b>3.1 Service Deployment .....</b>	<b>10</b>
<b>3.2 Service Orchestration.....</b>	<b>12</b>
<b>3.3 Cloud Service Management .....</b>	<b>14</b>
<b>3.3.1 Business Support .....</b>	<b>14</b>
<b>3.3.2 Provisioning and Configuration.....</b>	<b>15</b>
<b>3.3.3 Portability and Interoperability .....</b>	<b>15</b>
<b>3.4 Security .....</b>	<b>15</b>
<b>3.4.1 Cloud Service Model Perspectives.....</b>	<b>16</b>
<b>3.4.2 Implications of Cloud Deployment Models.....</b>	<b>16</b>
<b>3.4.3 Shared Security Responsibilities.....</b>	<b>16</b>
<b>3.5 Privacy .....</b>	<b>17</b>
<b>4. Cloud Taxonomy .....</b>	<b>18</b>
<b>Appendix A: Cloud Taxonomy Terms and Definitions .....</b>	<b>20</b>
<b>Appendix B: Examples of Cloud Services .....</b>	<b>24</b>
<b>Appendix C: Acronyms .....</b>	<b>26</b>
<b>Appendix D: References.....</b>	<b>27</b>

## List of Figures

Figure 1: The Conceptual Reference Model .....	3
Figure 2: Interactions between the Actors in Cloud Computing .....	4
Figure 3: Usage Scenario for Cloud Brokers .....	4
Figure 4: Usage Scenario for Cloud Carriers .....	5
Figure 5: Usage Scenario for Cloud Auditors .....	5
Figure 6: Example Services Available to a Cloud Consumer .....	6
Figure 7: Cloud Provider - Major Activities .....	7
Figure 8: Scope of Controls between Provider and Consumer .....	9
Figure 10: On-site Private Cloud .....	10
Figure 11: Out-sourced Private Cloud .....	11
Figure 12: On-site Community Cloud .....	11
Figure 13: Outsourced Community Cloud .....	12
Figure 14: Hybrid Cloud .....	12
Figure 15: Cloud Provider - Service Orchestration .....	13
Figure 16: Cloud Provider - Cloud Service Management .....	14
Figure 17: Cloud Taxonomy .....	19

## List of Tables

Table 1: Actors in Cloud Computing .....	4
--	---

## Executive Summary

The adoption of cloud computing into the US Government (USG) and its implementation depend upon a variety of technical and non-technical factors. A fundamental reference point, based on the NIST definition of Cloud Computing, is needed to describe an overall framework that can be used government-wide. This document presents the NIST Cloud Computing Reference Architecture (RA) and Taxonomy (Tax) that will accurately communicate the components and offerings of cloud computing. The guiding principles used to create the RA were 1) develop a vendor-neutral architecture that is consistent with the NIST definition and 2) develop a solution that does not stifle innovation by defining a prescribed technical solution. This solution will create a level playing field for industry to discuss and compare their cloud offerings with the US Government (USG). The resulting reference architecture and taxonomy for cloud computing was developed as an Actor/Role based model that lays out the central elements of cloud computing for Federal CIOs, Procurement Officials and IT Program Managers. The cloudscape is open and diversified and the accompanying taxonomy provides a means to describe it in an unambiguous manner. The RA is presented in two parts: a complete overview of the actors and their roles and the necessary architectural components for managing and providing cloud services such as service deployment, service orchestration, cloud service management, security and privacy. The Taxonomy is presented in its own section and appendices are dedicated to terms and definitions and examples of cloud services.

The *Overview* of the Reference Architecture describes five major actors with their roles & responsibilities using the newly developed Cloud Computing Taxonomy. The five major participating actors are the *Cloud Consumer*, *Cloud Provider*, *Cloud Broker*, *Cloud Auditor* and *Cloud Carrier*. These core individuals have key roles in the realm of cloud computing. For example, a Cloud Consumer is an individual or organization that acquires and uses cloud products and services. The purveyor of products and services is the Cloud Provider. Because of the possible service offerings (Software, Platform or Infrastructure) allowed for by the cloud provider, there will be a shift in the level of responsibilities for some aspects of the scope of control, security and configuration. The Cloud Broker acts as the intermediate between consumer and provider and will help consumers through the complexity of cloud service offerings and may also create value-added cloud services as well. The Cloud Auditor provides a valuable inherent function for the government by conducting the independent performance and security monitoring of cloud services. The Cloud Carrier is the organization who has the responsibility of transferring the data akin to the power distributor for the electric grid.

The *Architectural Components* of the Reference Architecture describes the important aspects of service deployment and service orchestration. The overall service management of the cloud is acknowledged as an important element in the scheme of the architecture. Business Support mechanisms are in place to recognize customer management issues like contracts, accounting and pricing and are vital to cloud computing. A discussion on Provisioning and Configuration points out the requirements for cloud systems to be available as needed, metered and have proper SLA management in place. Portability and Interoperability issues for data, systems and services are crucial factors facing consumers in adopting the cloud are also undertaken here. Consumers need confidence in moving their data and services across multiple cloud environments.

As a major architectural component of the cloud, Security and Privacy concerns need to be addressed and there needs to be a level of confidence and trust in order to create an atmosphere of acceptance in the cloud's ability to provide a trustworthy and reliable system. Security responsibilities, security consideration for different cloud service models and deployment models are also discussed.

## 1. Introduction

### 1.1 Background

The National Institute of Standards and Technology (NIST) has been designated by Federal Chief Information Officer (CIO) Vivek Kundra with technical leadership for US government (USG) agency efforts related to the adoption and development of cloud computing standards. The goal is to accelerate the federal government's adoption of secure and effective cloud computing to reduce costs and improve services. The NIST strategy is to build a USG Cloud Computing Technology Roadmap which focuses on the highest priority USG cloud computing security, interoperability and portability requirements, and to lead efforts to develop standards and guidelines in close consultation and collaboration with standards bodies, the private sector, and other stakeholders.

The NIST cloud computing program was formally launched in November 2010 to support the federal government effort to incorporate cloud computing as a replacement for, or enhancement to, traditional information system and application models where appropriate. The NIST cloud computing program operates in coordination with other USG-wide cloud computing efforts (CIO Council/ISIMC, etc.) and is integrated with the Federal 25-point IT Management Reform Plan<sup>1</sup> and Federal Cloud Computing Strategy<sup>2</sup>. NIST has created the following working groups in order to provide a technically-oriented strategy and standards-based guidance for the federal cloud computing implementation effort:

Cloud Computing Target Business Use Cases Working Group  
Cloud Computing Reference Architecture and Taxonomy Working Group  
Cloud Computing Standards Roadmap Working Group  
Cloud Computing SAJACC Working Group  
Cloud Computing Security Working Group

### 1.2 Objectives

The NIST cloud computing definition [1] is widely accepted as a valuable contribution toward providing a clear understanding of cloud computing technologies and cloud services. It provides a simple and unambiguous taxonomy of three service models available to cloud consumers: *cloud software as a service* (SaaS), *cloud platform as a service* (PaaS), and *cloud infrastructure as a service* (IaaS). It also summarizes four deployment models describing how the computing infrastructure that delivers these services can be shared: *private cloud*, *community cloud*, *public cloud*, and *hybrid cloud*. Finally, the NIST definition also provides a unifying view of five essential characteristics that all cloud services exhibit: *on-demand self-service*, *broad network access*, *resource pooling*, *rapid elasticity*, and *measured service*.

These services and their delivery are at the core of cloud computing. In the cloud computing model, the primary focus is a more economic method of providing higher quality and faster services at a lower cost to the users. In the traditional IT service delivery model, there is a large emphasis on procuring, maintaining and operating the necessary hardware and related infrastructure. The cloud computing model enables CIOs, IT project managers and procurement officials to direct their attention to innovative service creation for the customers.

In order to have successful service delivery, the USG needs to ensure the reliability in the delivery of products and processes. By ensuring durable and proper standards in place for cloud computing in security, data portability and service interoperability, the USG will have the additional confidence needed

<sup>1</sup>Office of Management and Budget, U.S. Chief Information Officer Vivek Kundra, “25 Point Implementation Plan to Reform Federal Information Technology Management”, December 2010. <http://www.cio.gov/documents/25-Point-Implementation-Plan-to-Reform-Federal%20IT.pdf>

<sup>2</sup>Office of Management and Budget, U.S. Chief Information Officer Vivek Kundra, “Federal Cloud Computing Strategy”, February 2011. <http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf>

to move their applications into the cloud. The necessary standards will also promote an even playing field among cloud service providers and give the cloud service consumers a number of different options in the marketplace and the confidence that their data and applications will operate on any cloud.

Standards for cloud computing are the overall goal of the NIST cloud computing program; the logical step to take after the formation of the NIST cloud computing definition is to create an intermediate reference point from where one can frame the rest of the discussion about cloud computing and begin to identify sections in the reference architecture in which standards are either required, useful or optional. The NIST cloud computing reference architecture presented in this document is a logical extension to the NIST cloud computing definition. It is a generic high-level conceptual model that is an effective tool for discussing the requirements, structures, and operations of cloud computing. The model is not tied to any specific vendor products, services or reference implementation, nor does it define prescriptive solutions that inhibit innovation. It defines a set of actors, activities and functions that can be used in the process of developing cloud computing architectures, and relates to a companion cloud computing taxonomy. The reference architecture contains a set of views and descriptions that are the basis for discussing the characteristics, uses and standards for cloud computing. This actor/role based model is intended to serve the expectations of the stakeholders by allowing them to understand the overall view of roles and responsibilities in order to assess and assign risk.

The NIST cloud computing reference architecture focuses on the requirements of “what” cloud services provide, *not* a “how to” design solution and implementation. The reference architecture is intended to facilitate the understanding of the operational intricacies in cloud computing. It does not represent the system architecture of a specific cloud computing system; instead it is a tool for describing, discussing, and developing a system-specific architecture using a common framework of reference.

The design of the NIST cloud computing reference architecture serves the following objectives: to illustrate and understand the various cloud services in the context of an overall cloud computing conceptual model; to provide a technical reference to USG agencies and other consumers to understand, discuss, categorize and compare cloud services; and to facilitate the analysis of candidate standards for security, interoperability, and portability and reference implementations.

### **1.3 How This Report Was Produced**

The NIST cloud computing reference architecture project team has surveyed and completed an initial analysis of existing cloud computing reference models proposed by cloud organizations, vendors and federal agencies. Based on available information, the project team developed a strawman model of architectural concepts. This effort has leveraged the collaborative process from the NIST cloud computing reference architecture and taxonomy working group that was active between November 2010 and April 2011. This process involves broad participation from the industry, academic, standards development organizations (SDOs), and private and public sector cloud adopters. The project team has iteratively revised the reference model by incorporating comments and feedback received from the working group. This document reports the first edition of the NIST cloud computing reference architecture and taxonomy.

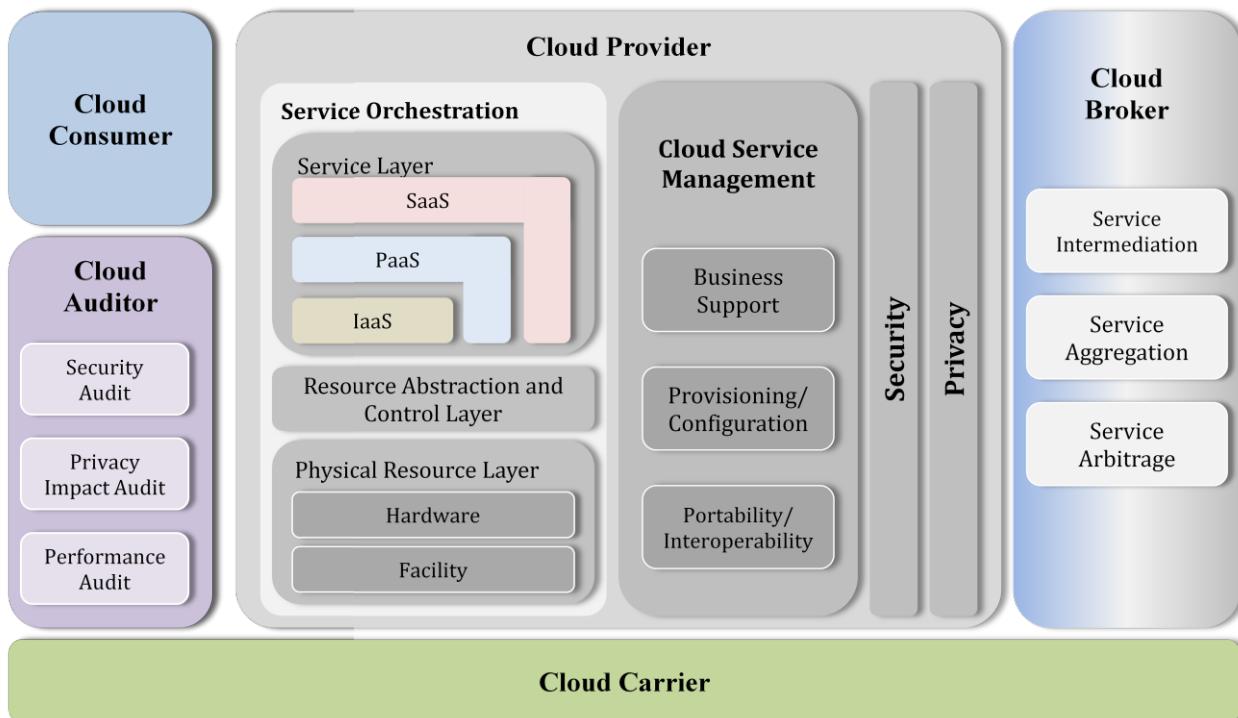
### **1.4 Structure of This Report**

The remainder of this document is organized as follows: Section 2 presents the overview of the NIST cloud computing reference architecture, lists the major actors and discusses the interactions among the actors. Section 3 drills down the details of the architectural components in the reference model. Section 4 depicts the associated taxonomy. The document also includes supporting materials in the appendices. Appendix A lists the terms and definitions appearing in the taxonomy. Appendix B includes some examples of cloud services. Appendix C and D list the acronyms and references used in the document, respectively.

## 2. Cloud Computing Reference Architecture: An Overview

### 2.1 The Conceptual Reference Model

Figure 1 presents an overview of the NIST cloud computing reference architecture, which identifies the major actors, their activities and functions in cloud computing. The diagram depicts a generic high-level architecture and is intended to facilitate the understanding of the requirements, uses, characteristics and standards of cloud computing.

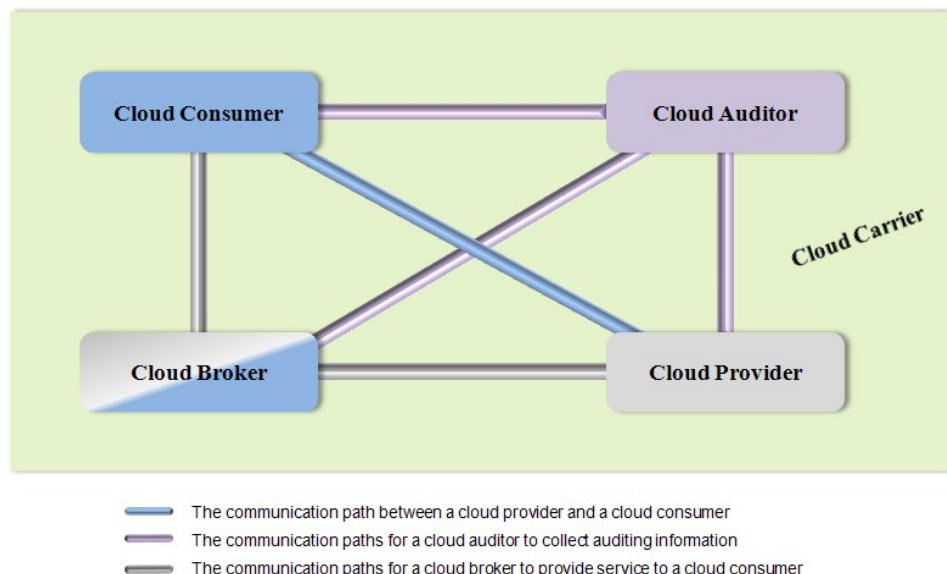


**Figure 1: The Conceptual Reference Model**

As shown in Figure 1, the NIST cloud computing reference architecture defines five major actors: *cloud consumer*, *cloud provider*, *cloud carrier*, *cloud auditor* and *cloud broker*. Each actor is an entity (a person or an organization) that participates in a transaction or process and/or performs tasks in cloud computing. Table 1 briefly lists the actors defined in the NIST cloud computing reference architecture. The general activities of the actors are discussed in the remainder of this section, while the details of the architectural elements are discussed in Section 3.

Figure 2 illustrates the interactions among the actors. A cloud consumer may request cloud services from a cloud provider directly or via a cloud broker. A cloud auditor conducts independent audits and may contact the others to collect necessary information. The details will be discussed in the following sections and presented in increasing level of details in successive diagrams.

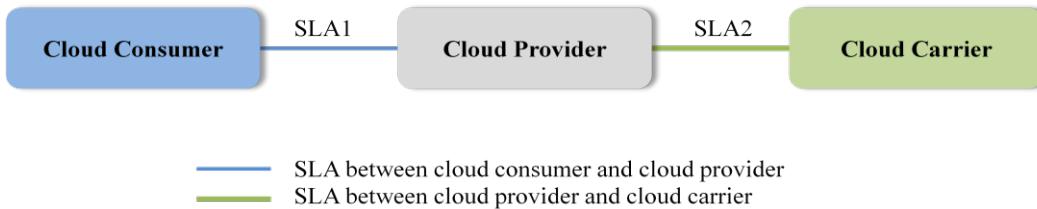
Actor	Definition
<b>Cloud Consumer</b>	A person or organization that maintains a business relationship with, and uses service from, <i>Cloud Providers</i> .
<b>Cloud Provider</b>	A person, organization, or entity responsible for making a service available to interested parties.
<b>Cloud Auditor</b>	A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
<b>Cloud Broker</b>	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between <i>Cloud Providers</i> and <i>Cloud Consumers</i> .
<b>Cloud Carrier</b>	An intermediary that provides connectivity and transport of cloud services from <i>Cloud Providers</i> to <i>Cloud Consumers</i> .

**Table 1: Actors in Cloud Computing****Figure 2: Interactions between the Actors in Cloud Computing**

- Example Usage Scenario 1:** A cloud consumer may request service from a cloud broker instead of contacting a cloud provider directly. The cloud broker may create a new service by combining multiple services or by enhancing an existing service. In this example, the actual cloud providers are invisible to the cloud consumer and the cloud consumer interacts directly with the cloud broker.

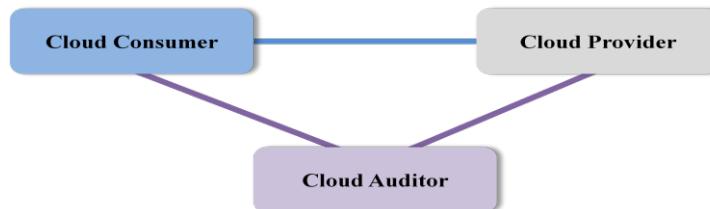
**Figure 3: Usage Scenario for Cloud Brokers**

- **Example Usage Scenario 2:** Cloud carriers provide the connectivity and transport of cloud services from cloud providers to cloud consumers. As illustrated in Figure 4, a cloud provider participates in and arranges for two unique service level agreements (SLAs), one with a cloud carrier (e.g. SLA2) and one with a cloud consumer (e.g. SLA1). A cloud provider arranges service level agreements (SLAs) with a cloud carrier and may request dedicated and encrypted connections to ensure the cloud services are consumed at a consistent level according to the contractual obligations with the cloud consumers. In this case, the provider may specify its requirements on capability, flexibility and functionality in SLA2 in order to provide essential requirements in SLA1.



**Figure 4: Usage Scenario for Cloud Carriers**

- **Example Usage Scenario 3:** For a cloud service, a cloud auditor conducts independent assessments of the operation and security of the cloud service implementation. The audit may involve interactions with both the Cloud Consumer and the Cloud Provider.



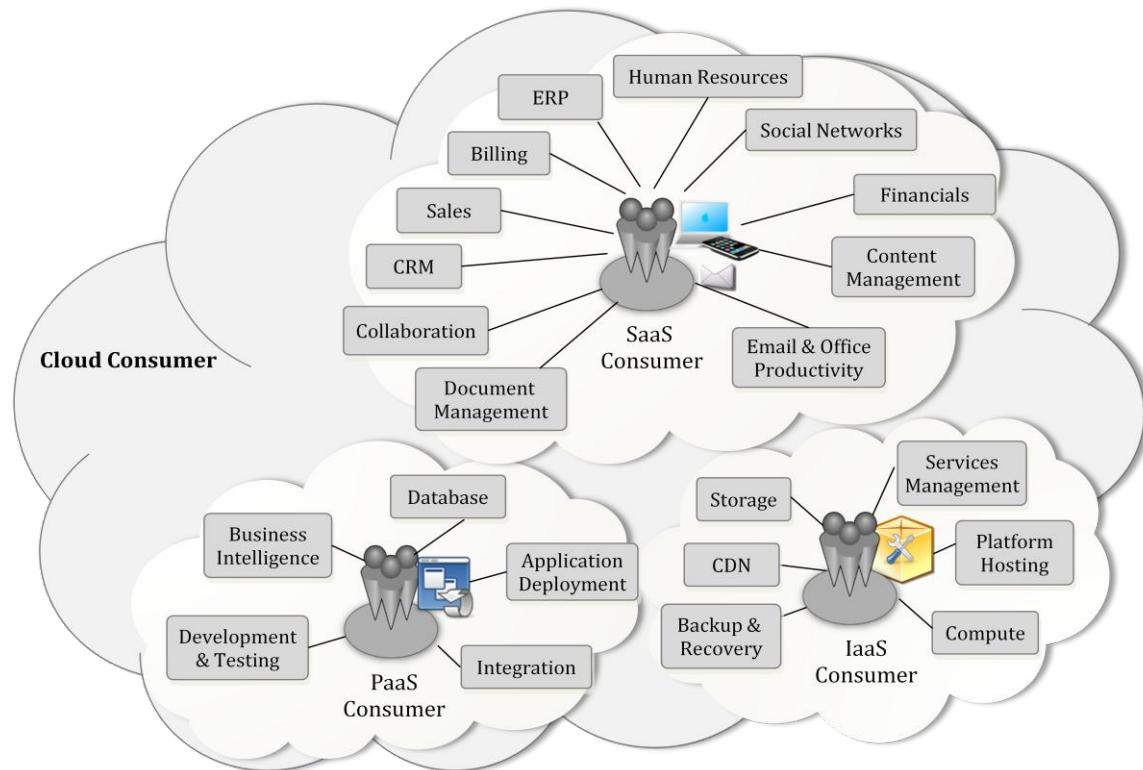
**Figure 5: Usage Scenario for Cloud Auditors**

## 2.2 Cloud Consumer

The cloud consumer is the principal stakeholder for the cloud computing service. A cloud consumer represents a person or organization that maintains a business relationship with, and uses the service from a cloud provider. A cloud consumer browses the service catalog from a cloud provider, requests the appropriate service, sets up service contracts with the cloud provider, and uses the service. The cloud consumer may be billed for the service provisioned, and needs to arrange payments accordingly.

Cloud consumers need SLAs to specify the technical performance requirements fulfilled by a cloud provider. SLAs can cover terms regarding the quality of service, security, remedies for performance failures. A cloud provider may also list in the SLAs a set of promises explicitly not made to consumers, i.e. limitations, and obligations that cloud consumers must accept. A cloud consumer can freely choose a cloud provider with better pricing and more favorable terms. Typically a cloud provider's pricing policy and SLAs are non-negotiable, unless the customer expects heavy usage and might be able to negotiate for better contracts. [2].

Depending on the services requested, the activities and usage scenarios can be different among cloud consumers. Figure 6 presents some example cloud services available to a cloud consumer (For details, see Appendix B: Examples of Cloud Services) [13].



**Figure 6: Example Services Available to a Cloud Consumer**

SaaS applications in the cloud and made accessible via a network to the SaaS consumers. The consumers of SaaS can be organizations that provide their members with access to software applications, end users who directly use software applications, or software application administrators who configure applications for end users. SaaS consumers can be billed based on the number of end users, the time of use, the network bandwidth consumed, the amount of data stored or duration of stored data.

Cloud consumers of PaaS can employ the tools and execution resources provided by cloud providers to develop, test, deploy and manage the applications hosted in a cloud environment. PaaS consumers can be application developers who design and implement application software, application testers who run and test applications in cloud-based environments, application deployers who publish applications into the cloud, and application administrators who configure and monitor application performance on a platform. PaaS consumers can be billed according to processing, database storage and network resources consumed by the PaaS application, and the duration of the platform usage.

Consumers of IaaS have access to virtual computers, network-accessible storage, network infrastructure components, and other fundamental computing resources on which they can deploy and run arbitrary software. The consumers of IaaS can be system developers, system administrators and IT managers who are interested in creating, installing, managing and monitoring services for IT infrastructure operations. IaaS consumers are provisioned with the capabilities to access these computing resources, and are billed according to the amount or duration of the resources consumed, such as CPU hours used by virtual computers, volume and duration of data stored, network bandwidth consumed, number of IP addresses used for certain intervals..

### 2.3 Cloud Provider

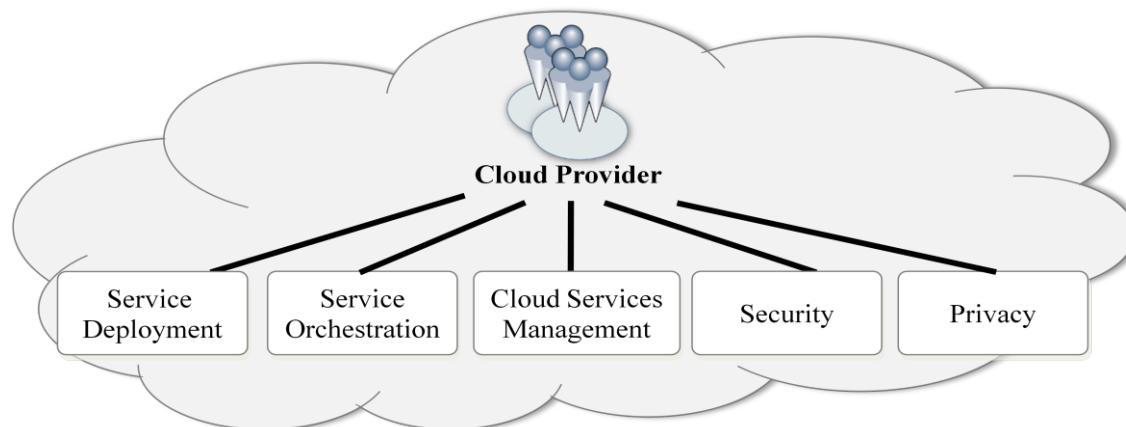
A cloud provider is a person, an organization; it is the entity responsible for making a service available to interested parties. A Cloud Provider acquires and manages the computing infrastructure required for providing the services, runs the cloud software that provides the services, and makes arrangement to deliver the cloud services to the Cloud Consumers through network access.

For Software as a Service, the cloud provider deploys, configures, maintains and updates the operation of the software applications on a cloud infrastructure so that the services are provisioned at the expected service levels to cloud consumers. The provider of SaaS assumes most of the responsibilities in managing and controlling the applications and the infrastructure, while the cloud consumers have limited administrative control of the applications.

For PaaS, the Cloud Provider manages the computing infrastructure for the platform and runs the cloud software that provides the components of the platform, such as runtime software execution stack, databases, and other middleware components. The PaaS Cloud Provider typically also supports the development, deployment and management process of the PaaS Cloud Consumer by providing tools such as integrated development environments (IDEs), development version of cloud software, software development kits (SDKs), deployment and management tools. The PaaS Cloud Consumer has control over the applications and possibly some the hosting environment settings, but has no or limited access to the infrastructure underlying the platform such as network, servers, operating systems (OS), or storage.

For IaaS, the Cloud Provider acquires the physical computing resources underlying the service, including the servers, networks, storage and hosting infrastructure. The Cloud Provider runs the cloud software necessary to makes computing resources available to the IaaS Cloud Consumer through a set of service interfaces and computing resource abstractions, such as virtual machines and virtual network interfaces. The IaaS Cloud Consumer in turn uses these computing resources, such as a virtual computer, for their fundamental computing needs Compared to SaaS and PaaS Cloud Consumers, an IaaS Cloud Consumer has access to more fundamental forms of computing resources and thus has more control over the more software components in an application stack, including the OS and network. The IaaS Cloud Provider, on the other hand, has control over the physical hardware and cloud software that makes the provisioning of these infrastructure services possible, for example, the physical servers, network equipments, storage devices, host OS and hypervisors for virtualization.

A Cloud Provider's activities can be described in five major areas, as shown in Figure 7, a cloud provider conducts its activities in the areas of *service deployment*, *service orchestration*, *cloud service management*, *security*, and *privacy*. The details are discussed in Section 3.



**Figure 7: Cloud Provider - Major Activities**

## 2.4 Cloud Auditor

A cloud auditor is a party that can perform an independent examination of cloud service controls with the intent to express an opinion thereon. Audits are performed to verify conformance to standards through review of objective evidence. A cloud auditor can evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance, etc.

Auditing is especially important for federal agencies as “agencies should include a contractual clause enabling third parties to assess security controls of cloud providers” [4] (by Vivek Kundra, *Federal Cloud Computing Strategy, Feb. 2011.*). Security controls [3] are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information. For security auditing, a cloud auditor can make an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to the security requirements for the system. The security auditing should also include the verification of the compliance with regulation and security policy. For example, an auditor can be tasked with ensuring that the correct policies are applied to data retention according to relevant rules for the jurisdiction. The auditor may ensure that fixed content has not been modified and that the legal and business data archival requirements have been satisfied.

A privacy impact audit can help Federal agencies comply with applicable privacy laws and regulations governing an individual’s privacy, and to ensure confidentiality, integrity, and availability of an individual’s personal information at every stage of development and operation [5].

## 2.5 Cloud Broker

As cloud computing evolves, the integration of cloud services can be too complex for cloud consumers to manage. A cloud consumer may request cloud services from a cloud broker, instead of contacting a cloud provider directly. A cloud broker is an entity that manages the use, performance and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers.

In general, a cloud broker can provide services in three categories [9]:

- *Service Intermediation:* A cloud broker enhances a given service by improving some specific capability and providing value-added services to cloud consumers. The improvement can be managing access to cloud services, identity management, performance reporting, enhanced security, etc.
- *Service Aggregation:* A cloud broker combines and integrates multiple services into one or more new services. The broker provides data integration and ensures the secure data movement between the cloud consumer and multiple cloud providers.
- *Service Arbitrage:* Service arbitrage is similar to service aggregation except that the services being aggregated are not fixed. Service arbitrage means a broker has the flexibility to choose services from multiple agencies. The cloud broker, for example, can use a credit-scoring service to measure and select an agency with the best score.

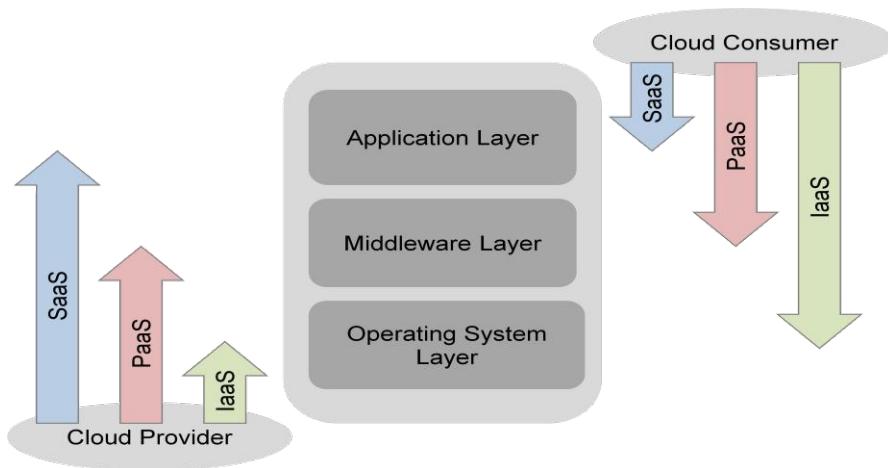
## 2.6 Cloud Carrier

A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers. Cloud carriers provide access to consumers through network, telecommunication and other access devices. For example, cloud consumers can obtain cloud services

through network access devices, such as computers, laptops, mobile phones, mobile Internet devices (MIDs), etc [1]. The distribution of cloud services is normally provided by network and telecommunication carriers or a *transport agent* [8], where a transport agent refers to a business organization that provides physical transport of storage media such as high-capacity hard drives. Note that a cloud provider will set up SLAs with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers, and may require the cloud carrier to provide dedicated and secure connections between cloud consumers and cloud providers.

## 2.7 Scope of Control between Provider and Consumer

The Cloud Provider and Cloud Consumer share the control of resources in a cloud system. As illustrated in Figure 8, different service models affect an organization's control over the computational resources and thus what can be done in a cloud system. The figure shows these differences using a classic software stack notation comprised of the application, middleware, and OS layers. This analysis of delineation of controls over the application stack helps understand the responsibilities of parties involved in managing the cloud application.



**Figure 8: Scope of Controls between Provider and Consumer**

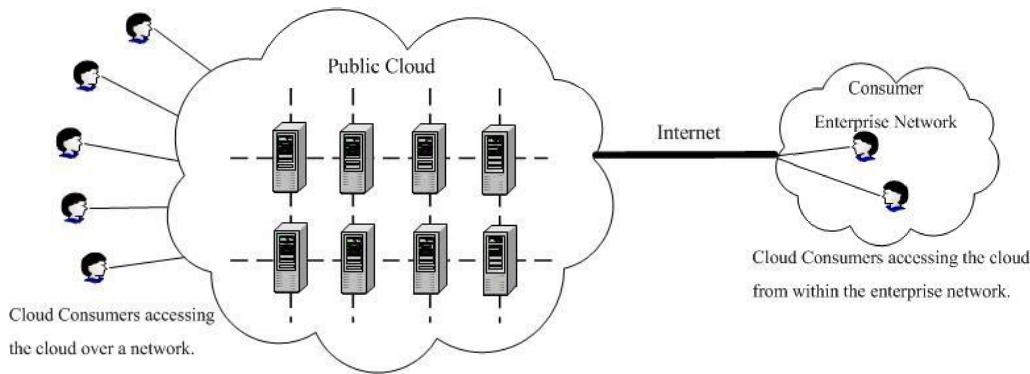
- The application layer includes software applications targeted at end users or programs. The applications are used by SaaS consumers, or installed/managed/ maintained by PaaS consumers, IaaS consumers, and SaaS providers.
- The middleware layer provides software building blocks (e.g., libraries, database, and Java virtual machine) for developing application software in the cloud. The middleware is used by PaaS consumers, installed/managed/maintained by IaaS consumers or PaaS providers, and hidden from SaaS consumers.
- The OS layer includes operating system and drivers, and is hidden from SaaS consumers and PaaS consumers. An IaaS cloud allows one or multiple guest OS's to run virtualized on a single physical host. Generally, consumers have broad freedom to choose which OS to be hosted among all the OS's that could be supported by the cloud provider. The IaaS consumers should assume full responsibility for the guest OS's, while the IaaS provider controls the host OS.

### 3. Cloud Computing Reference Architecture: Architectural Components

#### 3.1 Service Deployment

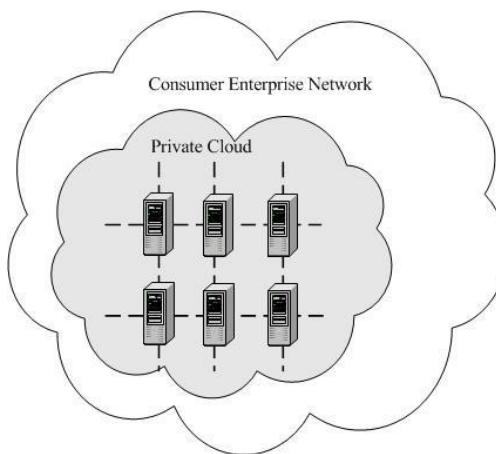
As identified in the NIST cloud computing definition [1], a cloud infrastructure may be operated in one of the following deployment models: public cloud, private cloud, community cloud, or hybrid cloud. The differences are based on how exclusive the computing resources are made to a Cloud Consumer.

A public cloud is one in which the cloud infrastructure and computing resources are made available to the general public over a public network. A public cloud is owned by an organization selling cloud services, and serves a diverse pool of clients. Figure 9 presents a simple view of a public cloud and its customers.

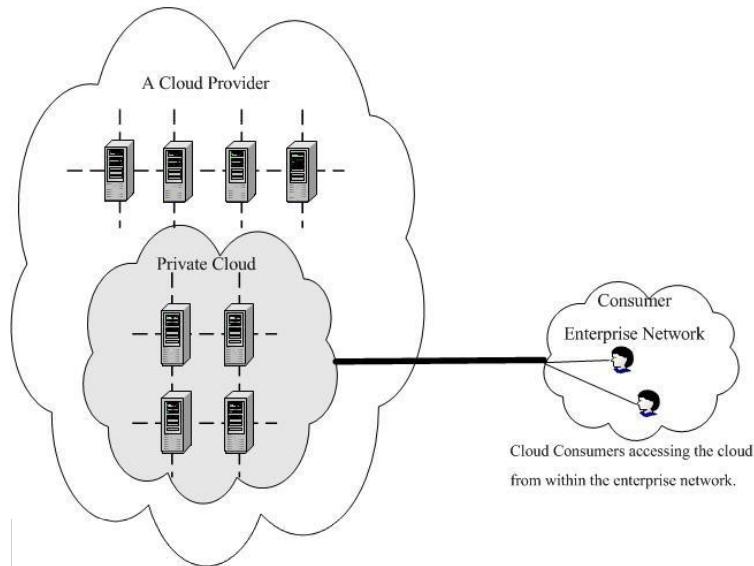


**Figure 9: Public Cloud**

A private cloud gives a single Cloud Consumer's organization the exclusive access to and usage of the infrastructure and computational resources. It may be managed either by the Cloud Consumer organization or by a third party, and may be hosted on the organization's premises (i.e. *on-site private clouds*) or outsourced to a hosting company (i.e. *outsourced private clouds*). Figure 10 and Figure 11 present an on-site private cloud and an outsourced private cloud, respectively.

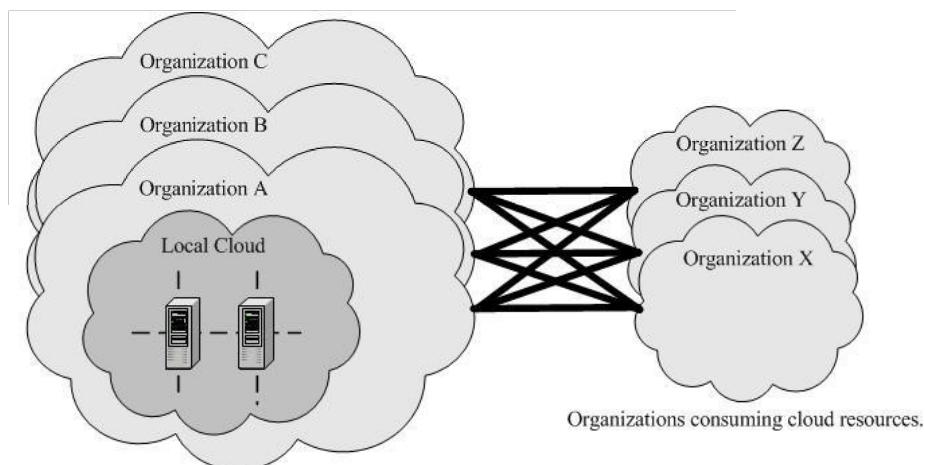


**Figure 10: On-site Private Cloud**

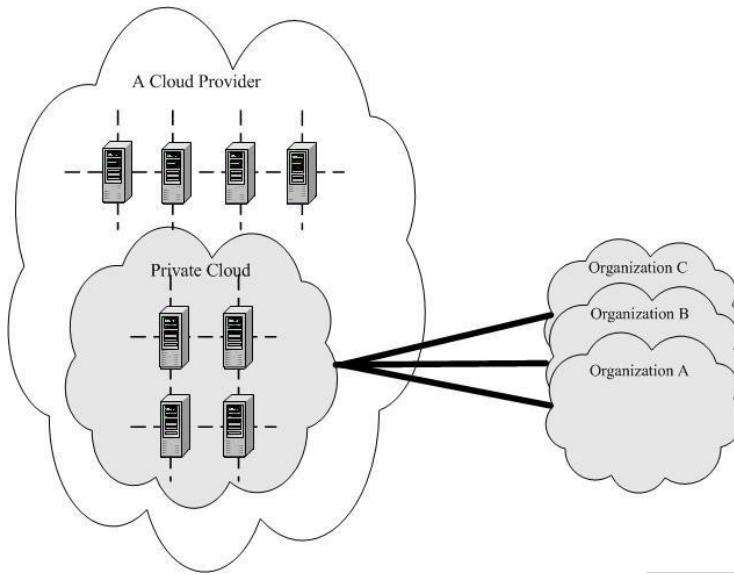


**Figure 11: Out-sourced Private Cloud**

A community cloud serves a group of Cloud Consumers which have shared concerns such as mission objectives, security, privacy and compliance policy, rather than serving a single organization as does a private cloud. Similar to private clouds, a community cloud may be managed by the organizations or by a third party, and may be implemented on customer premise (i.e. *on-site community cloud*) or outsourced to a hosting company (i.e. *outsourced community cloud*). Figure 12 depicts an on-site community cloud comprised of a number of participant organizations. A cloud consumer can access the local cloud resources, and also the resources of other participating organizations through the connections between the associated organizations. Figure 13 shows an outsourced community cloud, where the server side is outsourced to a hosting company. In this case, an outsourced community cloud builds its infrastructure off premise, and serves a set of organizations that request and consume cloud services.

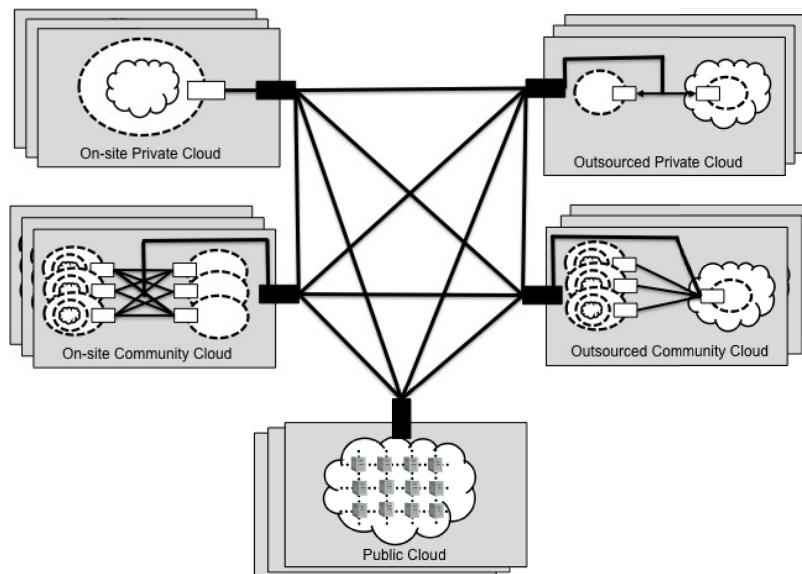


**Figure 12: On-site Community Cloud**



**Figure 13: Outsourced Community Cloud**

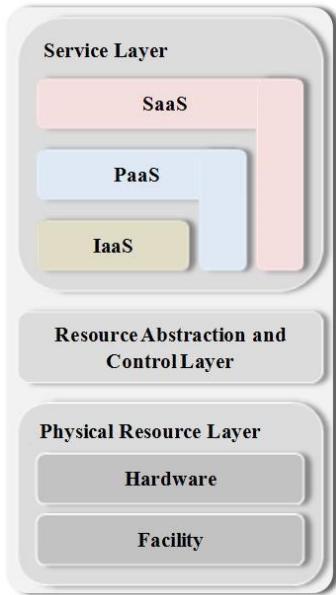
A hybrid cloud is a composition of two or more clouds (on-site private, on-site community, off-site private, off-site community or public) that remain as distinct entities but are bound together by standardized or proprietary technology that enables data and application portability. Figure 14 presents a simple view of a hybrid cloud that could be built with a set of clouds in the five deployment model variants.



**Figure 14: Hybrid Cloud**

### 3.2 Service Orchestration

*Service Orchestration* refers to the composition of system components to support the Cloud Providers activities in arrangement, coordination and management of computing resources in order to provide cloud services to Cloud Consumers. Figure 15 shows a generic stack diagram of this composition that underlies the provisioning of cloud services.



**Figure 15: Cloud Provider - Service Orchestration**

A three-layered model is used in this representation, representing the grouping of three types of system components Cloud Providers need to compose to deliver their services.

In the model shown in Figure 15, the top is the *service layer*, this is where Cloud Providers define interfaces for Cloud Consumers to access the computing services. Access interfaces of each of the three service models are provided in this layer. It is possible, though not necessary, that SaaS applications can be built on top of PaaS components and PaaS components can be built on top of IaaS components. The optional dependency relationships among SaaS, PaaS, and IaaS components are represented graphically as components stacking on each other; while the angling of the components represents that each of the service component can stand by itself. For example, a SaaS application can be implemented and hosted on virtual machines from an IaaS cloud or it can be implemented directly on top of cloud resources without using IaaS virtual machines.

The middle layer in the model is the *resource abstraction and control layer*. This layer contains the system components that Cloud Providers use to provide and manage access to the physical computing resources through software abstraction. Examples of *resource abstraction* components include software elements such as hypervisors, virtual machines, virtual data storage, and other computing resource abstractions. The resource abstraction needs to ensure efficient, secure, and reliable usage of the underlying physical resources. While virtual machine technology is commonly used at this layer, other means of providing the necessary software abstractions are also possible. The *control* aspect of this layer refers to the software components that are responsible for resource allocation, access control, and usage monitoring. This is the software fabric that ties together the numerous underlying physical resources and their software abstractions to enable resource pooling, dynamic allocation, and measured service. Various open source and proprietary cloud software are examples of this type of middleware.

The lowest layer in the stack is the *physical resource layer*, which includes all the physical computing resources. This layer includes hardware resources, such as computers (CPU and memory), networks (routers, firewalls, switches, network links and interfaces), storage components (hard disks) and other physical computing infrastructure elements. It also includes facility resources, such as heating, ventilation and air conditioning (HVAC), power, communications, and other aspects of the physical plant.

Following system architecture conventions, the horizontal positioning, i.e., the *layering*, in a model represents dependency relationships – the upper layer components are dependent on adjacent lower layer

to function. The resource abstraction and control layer exposes virtual cloud resources on top of the physical resource layer and supports the service layer where cloud services interfaces are exposed to Cloud Consumers, while Cloud Consumers do not have direct access to the physical resources.

### 3.3 Cloud Service Management

**Cloud Service Management** includes all of the service-related functions that are necessary for the management and operation of those services required by or proposed to cloud consumers. As illustrated in Figure 16, cloud service management can be described from the perspective of *business support*, *provisioning and configuration*, and from the perspective of *portability and interoperability* requirements.

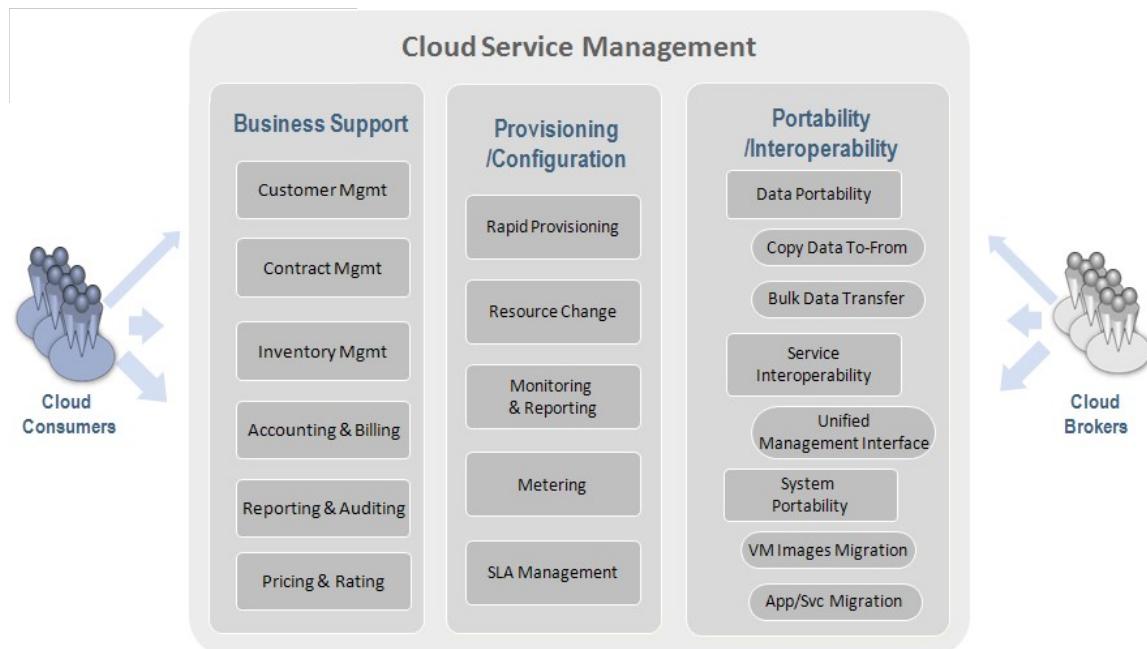


Figure 16: Cloud Provider - Cloud Service Management

#### 3.3.1 Business Support

*Business Support* entails the set of business-related services dealing with clients and supporting processes. It includes the components used to run business operations that are client-facing.

- *Customer management*: Manage customer accounts, open/close/terminate accounts, manage user profiles, manage customer relationships by providing points-of-contact and resolving customer issues and problems, etc.
- *Contract management*: Manage service contracts, setup/negotiate/close/terminate contract, etc.
- *Inventory Management*: Set up and manage service catalogs, etc.
- *Accounting and Billing*: Manage customer billing information, send billing statements, process received payments, track invoices, etc.
- *Reporting and Auditing*: Monitor user operations, generate reports, etc.

- *Pricing and Rating*: Evaluate cloud services and determine prices, handle promotions and pricing rules based on a user's profile, etc.

### 3.3.2 Provisioning and Configuration

- *Rapid provisioning*: Automatically deploying cloud systems based on the requested service/resources/capabilities.
- *Resource changing*: Adjusting configuration/resource assignment for repairs, upgrades and joining new nodes into the cloud.
- *Monitoring and Reporting*: Discovering and monitoring virtual resources, monitoring cloud operations and events and generating performance reports.
- *Metering*: Providing a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts).
- *SLA management*: Encompassing the SLA contract definition (basic schema with the QoS parameters), SLA monitoring and SLA enforcement according to defined policies.

### 3.3.3 Portability and Interoperability

The proliferation of cloud computing promises cost savings in technology infrastructure and faster software upgrades. The US government, along with other potential cloud computing customers, has a strong interest in moving to the cloud. However, the adoption of cloud computing depends greatly on how the cloud can address users' concerns on security, portability and interoperability. This section briefly discusses the requirement for portability and interoperability, with security addressed in Section 3.4.

For portability, prospective customers are interested to know whether they can move their data or applications across multiple cloud environments at low cost and minimal disruption. From an interoperability perspective, users are concerned about the capability to communicate between or among multiple clouds.

Cloud providers should provide mechanisms to support *data portability*, *service interoperability*, and *system portability* [8]. Data portability is the ability of cloud consumers to copy data objects into or out of a cloud or to use a disk for bulk data transfer. Service interoperability is the ability of cloud consumers to use their data and services across multiple cloud providers with a unified management interface. System portability allows the migration of a fully-stopped virtual machine instance or a machine image from one provider to another provider, or migrate applications and services and their contents from one service provider to another.

It should be noted that various cloud service models may have different requirements in related with portability and interoperability [35]. For example, IaaS requires the ability to migrate the data and run the applications on a new cloud. Thus, it is necessary to capture virtual machine images and migrate to new cloud providers which may use different virtualization technologies. Any provider-specific extensions to the VM images need to be removed or recorded upon being ported. While for SaaS, the focus is on data portability, and thus it is essential to perform data extractions and backups in a standard format.

## 3.4 Security

It is critical to recognize that security is a cross-cutting aspect of the architecture that spans across all layers of the reference model, ranging from physical security to application security. Therefore, security in cloud computing architecture concerns is not solely under the purview of the Cloud Providers, but also

Cloud Consumers and other relevant actors. Cloud-based systems still need to address security requirements such as authentication, authorization, availability, confidentiality, identity management, integrity, audit, security monitoring, incident response, and security policy management. While these security requirements are not new, we discuss cloud specific perspectives to help discuss, analyze and implement security in a cloud system.

### **3.4.1 Cloud Service Model Perspectives**

The three service models identified by the NIST cloud computing definition, i.e. SaaS, PaaS, and IaaS, present consumers with different types of service management operations and expose different entry points into cloud systems, which in turn also create different attacking surfaces for adversaries. Hence, it is important to consider the impact of cloud service models and their different issues in security design and implementation. For example, SaaS provides users with accessibility of cloud offerings using a network connection, normally over the Internet and through a Web browser. There has been an emphasis on Web browser security in SaaS cloud system security considerations [2]. Cloud Consumers of IaaS are provided with virtual machines (VMs) that are executed on hypervisors on the hosts, therefore, hypervisor security for achieving VM isolation has been studied extensively for IaaS Cloud Providers that use virtualization technologies.

### **3.4.2 Implications of Cloud Deployment Models**

The variations of cloud deployment models discussed in section 3.1 have important security implication as well. One way to look at the security implications from the deployment model perspective is the differing level of exclusivity of tenants in a deployment model. A private cloud is dedicated to one consumer organization, whereas a public cloud could have unpredictable tenants co-existing with each other, therefore, workload isolation is less of a security concern in a private cloud than in a public cloud. Another way to analyze the security impact of cloud deployment models is to use the concept of access boundaries as shown in [2]. For example, an on-site private cloud may or may not need additional boundary controllers at the cloud boundary when the private cloud is hosted on-site within the Cloud Consumer organization's network boundary, whereas an out-sourced private cloud tends to require the establishment of such perimeter protection at the boundary of the cloud.

### **3.4.3 Shared Security Responsibilities**

As discussed in Section 2.7, the Cloud Provider and the Cloud Consumer have differing degrees of control over the computing resources in a cloud system. Compared to traditional IT systems, where one organization has control over the whole stack of computing resources and the entire life-cycle of the systems, Cloud Providers and Cloud Consumers collaboratively design, build, deploy, and operate cloud-based systems. The split of control means both parties now share the responsibilities in providing adequate protections to the cloud-based systems. Security is a shared responsibility. Security controls, i.e., measures used to provide protections, need to be analyzed to determine which party is in a better position to implement. This analysis needs to include considerations from a service model perspective, where different service models imply different degrees of control between Cloud Providers and Cloud Consumers. For example, account management controls for initial system privileged users in IaaS scenarios are typically performed by the IaaS Provider whereas application user account management for the application deployed in an IaaS environment is typically not the provider's responsibility.

### 3.5 Privacy

Cloud providers should protect the assured, proper, and consistent collection, processing, communication, use and disposition of personal information (PI) and personally identifiable information (PII) in the cloud [14].

According to the Federal CIO Council [5], one of the Federal government's key business imperatives is to ensure the privacy of the collected personally identifiable information. PII is the information that can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc [6]. Though cloud computing provides a flexible solution for shared resources, software and information, it also poses additional privacy challenges to consumers using the clouds.

## 4. Cloud Taxonomy

Taxonomy is the science of categorization, or classification, of things based on a predefined system [22]. Typically, taxonomy contains a controlled vocabulary with a hierarchical tree-like structure.

Figure 17 presents the taxonomy associated with the cloud computing reference architecture discussed in this document. In the figure, a four-level taxonomy is presented to describe the key concepts about cloud computing.

- *Level 1: Role*, which indicates a set of obligations and behaviors as conceptualized by the associated actors in the context of cloud computing.
- *Level 2: Activity*, which entails the general behaviors or tasks associated to a specific role.
- *Level 3: Component*, which refer to the specific processes, actions, or tasks that must be performed to meet the objective of a specific activity.
- *Level 4: Sub-component*, which present a modular part of a component.

The companion controlled vocabulary is shown in Appendix A: Cloud Taxonomy Terms and Definitions.

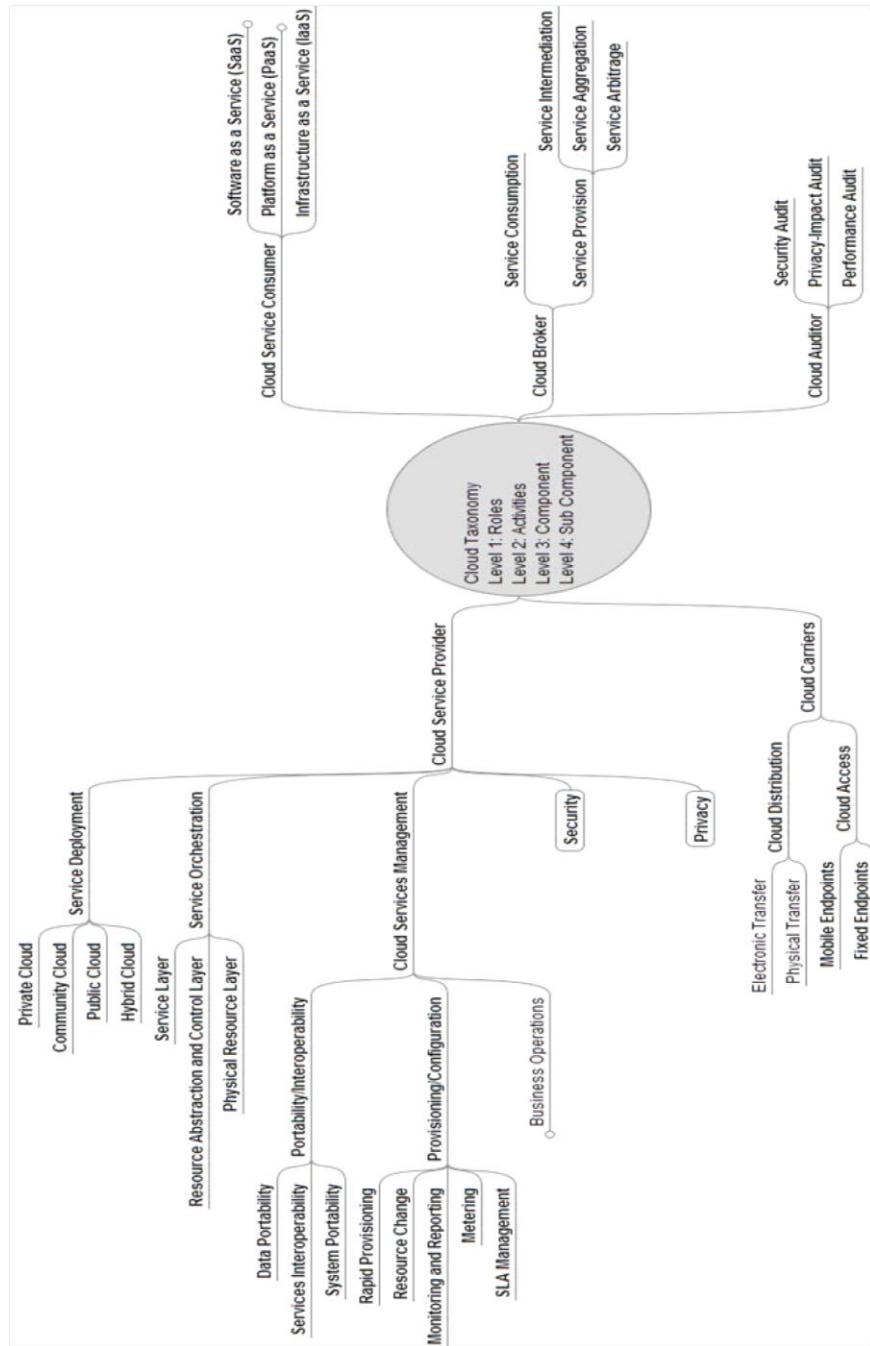


Figure 17: Cloud Taxonomy



**National Institute of  
Standards and Technology**  
U.S. Department of Commerce

Special Publication 500-291, Version 2

---

# **NIST Cloud Computing Standards Roadmap**

---

*NIST Cloud Computing Standards Roadmap Working Group  
NIST Cloud Computing Program  
Information Technology Laboratory*



**National Institute of Standards and Technology • U.S. Department of Commerce**

**NIST Special Publication 500-291,  
Version 2**

(Supersedes Version 1.0, July 2011)

**NIST Cloud Computing  
Standards Roadmap**

NIST Cloud Computing Standards

Roadmap Working Group

July 2013



**U. S. Department of Commerce**  
Penny Pritzker, Secretary

**National Institute of Standards and Technology**

Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

## Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in federal computer systems. This document reports on ITL's research, guidance, and outreach efforts in Information Technology and its collaborative activities with industry, government, and academic organizations.

**National Institute of Standards and Technology Special Publication 500-291 V2**

Natl. Inst. Stand. Technol. Spec. Publ. 500-291, 108 pages (May 24, 2013)

## DISCLAIMER

This document has been prepared by the National Institute of Standards and Technology (NIST) and describes standards research in support of the NIST Cloud Computing Program.

Certain commercial entities, equipment, or material may be identified in this document in order to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that these entities, materials, or equipment are necessarily the best available for the purpose.

## Acknowledgements

This document is an update of the first version, which was published in July 2011. It reflects the contributions and discussions by the membership of the NIST Cloud Computing Standards Roadmap Working Group, chaired by Michael Hogan and Annie Sokol of the Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce.

NIST SP 500-291, Version 2 has been collaboratively authored by the NIST Cloud Computing Standards Roadmap Working Group. As of the date of this publication, there are over one thousand Working Group participants from industry, academia, and government. Federal agency participants include NASA and the U.S. Departments of Agriculture, Commerce, Defense, Health & Human Services, Homeland Security, Justice, Transportation, Treasury, State, and Veterans Affairs.

NIST would like to acknowledge the specific contributions from the following Working Group members:

Alan Sill, Open Grid Forum	Michaela Iorga, NIST
Annie Sokol, NIST	Nancy Landreville, University of Maryland
Craig Lee, Open Grid Forum	P W Carey, Compliance Partners, LLC
David Harper, Johns Hopkins University	Paul Lipton, CA Technologies
Eugene Luster, U.S. Department of Defense	Richard Brackney, Microsoft
Frederic de Vaulx, NIST	Robert Bohn, NIST
Gary Massaferro, AlloyCloud, Inc.	Robert Marcus, Cloud Standards Customer Council
Gilbert Pilz, Oracle Corporation	Shin Adachi, NTT Multimedia Communications Labs
Jerry Smith, US Department of Defense	Steven McGee, SAW Concepts LLC
John Calhoon, Microsoft	Steven Woodward, Woodward Systems
John Messina, NIST	Sundararajan Ramanathan, Capgemini US Consulting
Michael Hogan, NIST	Winston Bumpus, DMTF, VMWare Inc.
Michael Stewart, Space and Naval Warfare Systems Command	

The NIST editors for this document were: Michael Hogan and Annie Sokol.

# TABLE OF CONTENTS

<b>1</b>	<b>EXECUTIVE SUMMARY .....</b>	<b>1</b>
<b>2</b>	<b>INTRODUCTION .....</b>	<b>5</b>
2.1	BACKGROUND.....	5
2.2	NIST CLOUD COMPUTING VISION .....	6
2.3	NIST CLOUD COMPUTING STANDARDS ROADMAP WORKING GROUP .....	7
2.4	HOW THIS REPORT WAS PRODUCED .....	7
<b>3</b>	<b>THE NIST DEFINITION OF CLOUD COMPUTING .....</b>	<b>8</b>
<b>4</b>	<b>CLOUD COMPUTING REFERENCE ARCHITECTURE.....</b>	<b>11</b>
4.1	OVERVIEW .....	11
4.2	CLOUD CONSUMER.....	14
4.3	CLOUD PROVIDER .....	16
4.3.1	SERVICE DEPLOYMENT.....	17
4.3.2	SERVICE ORCHESTRATION.....	18
4.3.3	CLOUD SERVICE MANAGEMENT .....	19
4.3.4	SECURITY.....	20
4.3.5	PRIVACY.....	21
4.4	CLOUD AUDITOR .....	23
4.5	CLOUD BROKER .....	23
4.6	CLOUD CARRIER.....	24
<b>5</b>	<b>CLOUD COMPUTING USE CASES.....</b>	<b>25</b>
5.1	BUSINESS USE CASES .....	25
5.2	TECHNICAL USE CASES .....	26
5.3	DEPLOYMENT SCENARIO PERSPECTIVE .....	26
<b>6</b>	<b>CLOUD COMPUTING STANDARDS .....</b>	<b>32</b>
6.1	INFORMATION AND COMMUNICATION TECHNOLOGIES (IT) STANDARDS LIFE CYCLE .....	32
6.2	THE ROLE OF CONFORMITY ASSESSMENT TO STANDARDS .....	33
6.2.1	CONFORMITY ASSESSMENT ACTIVITIES .....	34
6.2.2	GOVERNMENT USE OF CONFORMITY ASSESSMENT SYSTEMS .....	35
6.2.3	VISUALIZATION OF CONFORMITY ASSESSMENT PROCESSES .....	36
6.2.4	CURRENT STATE OF CONFORMITY ASSESSMENT IN CLOUD COMPUTING .....	38
6.3	CATEGORIZING THE STATUS OF STANDARDS .....	39
6.4	CLOUD COMPUTING STANDARDS FOR INTEROPERABILITY AND PORTABILITY .....	40
6.4.1	CLOUD STANDARDS FOR INTEROPERABILITY .....	40
6.4.2	CLOUD COMPUTING STANDARDS FOR PORTABILITY .....	42
6.4.3	SUMMARY ON INTEROPERABILITY AND PORTABILITY .....	43
6.5	CLOUD COMPUTING STANDARDS FOR SECURITY .....	44
6.6	CLOUD COMPUTING STANDARDS FOR PERFORMANCE .....	47
6.6.1	CLOUD STANDARDS FOR SERVICE AGREEMENTS .....	48
6.6.2	CLOUD STANDARDS FOR MONITORING.....	49
6.7	CLOUD COMPUTING STANDARDS FOR ACCESSIBILITY .....	49
<b>7</b>	<b>CLOUD COMPUTING STANDARDS MAPPING .....</b>	<b>51</b>
7.1	SECURITY STANDARDS MAPPING .....	52
7.2	INTEROPERABILITY STANDARDS MAPPING .....	58
7.3	PORTABILITY STANDARDS MAPPING .....	59

## NIST CLOUD COMPUTING STANDARDS ROADMAP

7.4 PERFORMANCE STANDARDS MAPPING.....	60
7.5 ACCESSIBILITY STANDARDS MAPPING.....	61
<b>8 ANALYZING USE CASES TO IDENTIFY STANDARDS GAPS .....</b>	<b>62</b>
8.1 USE CASE: CREATING, ACCESSING, UPDATING, DELETING DATA OBJECTS IN CLOUD SYSTEMS .....	62
8.2 USE CASE: MOVING VMS, VIRTUAL APPLIANCES, SERVICES, AND APPLIANCES BETWEEN CLOUDS .....	63
8.3 USE CASE: SELECTING THE BEST IAAS CLOUD VENDOR, PUBLIC OR PRIVATE .....	63
8.4 USE CASE: PORTABLE TOOLS FOR MONITORING AND MANAGING CLOUD SYSTEMS .....	63
8.5 USE CASE: MOVING DATA BETWEEN CLOUD SYSTEMS .....	64
8.6 USE CASE: SINGLE SIGN-ON ACCESS TO MULTIPLE CLOUD SYSTEMS .....	65
8.7 USE CASE: ORCHESTRATED PROCESSES ACROSS CLOUD SYSTEMS AND ENTERPRISE SYSTEMS .....	65
8.8 USE CASE: DISCOVERING CLOUD RESOURCES .....	66
8.9 USE CASE: EVALUATING SLAS AND PENALTIES.....	67
8.10 USE CASE: AUDITING CLOUD SYSTEMS .....	67
8.11 END-TO-END: CLOUD RESOURCE MANAGEMENT USE CASE.....	68
<b>9 USG PRIORITIES TO FILL CLOUD COMPUTING STANDARDS GAPS .....</b>	<b>69</b>
9.1 AREAS OF STANDARDIZATION GAPS.....	69
9.1.1 SAAS FUNCTIONAL INTERFACES.....	70
9.1.2 SAAS SELF-SERVICE MANAGEMENT INTERFACES.....	70
9.1.3 PAAS FUNCTIONAL INTERFACES.....	70
9.1.4 BUSINESS SUPPORT, PROVISIONING AND CONFIGURATION.....	70
9.1.5 SECURITY.....	71
9.1.6 ACCESSIBILITY.....	71
9.2 STANDARDIZATION PRIORITIES BASED ON USG CLOUD COMPUTING ADOPTION PRIORITIES	72
9.2.1 SECURITY AUDITING AND COMPLIANCE.....	72
9.2.2 IDENTITY AND ACCESS MANAGEMENT .....	73
9.2.3 SAAS APPLICATION SPECIFIC DATA AND METADATA .....	73
9.2.4 RESOURCE DESCRIPTION AND DISCOVERY.....	73
9.2.5 SUMMARY OF STANDARDIZATION GAPS AND STANDARDIZATION PRIORITIES .....	74
<b>10 CONCLUSIONS AND RECOMMENDATIONS.....</b>	<b>76</b>
10.1 CONCLUSIONS.....	76
10.2 RECOMMENDATION TO USG AGENCIES TO HELP ACCELERATE THE DEVELOPMENT AND USE OF CLOUD COMPUTING STANDARDS .....	76
<b>11 BIBLIOGRAPHY.....</b>	<b>78</b>
<b>12 APPENDIX A – NIST FEDERAL INFORMATION PROCESSING STANDARDS AND SPECIAL PUBLICATIONS RELEVANT TO CLOUD COMPUTING .....</b>	<b>80</b>
<b>13 APPENDIX B – DEFINITIONS.....</b>	<b>81</b>
<b>14 APPENDIX C – ACRONYMS .....</b>	<b>86</b>
<b>15 APPENDIX D – STANDARDS DEVELOPING ORGANIZATIONS .....</b>	<b>89</b>
<b>16 APPENDIX E – CONCEPTUAL MODELS AND ARCHITECTURES.....</b>	<b>97</b>
<b>17 APPENDIX F – EXAMPLES OF USG CRITERIA FOR SELECTION OF STANDARDS .....</b>	<b>98</b>

# LIST OF FIGURES

FIGURE 1 – CLOUD ACTORS .....	12
FIGURE 2 – INTERACTIONS BETWEEN THE ACTORS IN CLOUD COMPUTING .....	13
FIGURE 3 – EXAMPLE OF SERVICES AVAILABLE TO A CLOUD CONSUMER .....	15
FIGURE 4 – CLOUD PROVIDER: MAJOR ACTIVITIES .....	16
FIGURE 5 – CLOUD PROVIDER: SERVICE ORCHESTRATION.....	18
FIGURE 6 – CLOUD PROVIDER: CLOUD SERVICE MANAGEMENT.....	20
FIGURE 7 – HIGH-LEVEL GENERIC SCENARIOS .....	27
FIGURE 8 – IT STANDARDS LIFE CYCLE .....	33
FIGURE 9 – CONFORMITY ASSESSMENT INFRASTRUCTURE .....	36
FIGURE 10 – ACCREDITATION PROCESS .....	37
FIGURE 11 – ASSESSMENT PROCESS .....	38
FIGURE 12 – THE COMBINED CONCEPTUAL REFERENCE DIAGRAM .....	51
FIGURE 13 – DoD DISR STANDARDS SELECTION PROCESS .....	102

# LIST OF TABLES

TABLE 1 – CLOUD CONSUMER AND CLOUD PROVIDER .....	14
TABLE 2 – DEPLOYMENT CASES FOR HIGH LEVEL SCENARIOS .....	28
TABLE 3 – SCENARIOS AND TECHNICAL REQUIREMENTS .....	31
TABLE 4 – STANDARDS MATURITY MODEL .....	39
TABLE 5 – SECURITY STANDARDS: AUTHENTICATION AND AUTHORIZATION .....	52
TABLE 6 – SECURITY STANDARDS: CONFIDENTIALITY .....	53
TABLE 7 – SECURITY STANDARDS: INTEGRITY .....	53
TABLE 8 – SECURITY STANDARDS: IDENTITY MANAGEMENT .....	54
TABLE 9 – SECURITY STANDARDS: SECURITY MONITORING & INCIDENT RESPONSE .....	55
TABLE 10 – SECURITY STANDARDS: SECURITY CONTROLS .....	56
TABLE 11 – SECURITY STANDARDS: SECURITY POLICY MANAGEMENT .....	57
TABLE 12 – SECURITY STANDARDS: AVAILABILITY .....	57
TABLE 13 – INTEROPERABILITY STANDARDS .....	58
TABLE 14 – PORTABILITY STANDARDS .....	59
TABLE 15 – PERFORMANCE STANDARDS .....	60
TABLE 16 – ACCESSIBILITY STANDARDS .....	61
TABLE 17 – AREAS OF STANDARDIZATION GAPS AND STANDARDIZATION PRIORITIES .....	75
TABLE 18 – DOD SELECTION CRITERIA AND DESCRIPTION SUMMARY .....	100
TABLE 19 – DOD STANDARDS SOURCES PREFERENCES .....	101

## Foreword

This is the second edition of the NIST Cloud Computing Standards Roadmap, which has been developed by the members of the public NIST Cloud Computing Standards Roadmap Working Group. This edition includes updates to the information on portability, interoperability, and security standards in the first edition and adds new information on accessibility and performance standards. Also new in this edition is information on the role of conformity assessment in support of voluntary consensus standards. Analyzing typical government use cases (see Section 8), U.S. Government priorities and gaps in cloud computing voluntary consensus standards are identified in this edition and the previous edition. This information is intended for use by federal agencies and other stakeholders to help plan their participation in voluntary consensus standards development and related conformity assessment activities, which can help to accelerate the agencies' secure adoption of cloud computing.

## **1 EXECUTIVE SUMMARY**

The National Institute of Standards and Technology (NIST) has been designated by the Federal Chief Information Officer (CIO) to accelerate the federal government's secure adoption of cloud computing by leading efforts to identify existing standards and guidelines. Where standards are needed, NIST works closely with U.S. industry, standards developers, other government agencies, and leaders in the global standards community to develop standards that will support secure cloud computing.

Consistent with NIST's mission,<sup>1</sup> the NIST Cloud Computing Program has developed a *USG Cloud Computing Technology Roadmap*, as one of many mechanisms in support of United States Government (USG) secure and effective adoption of the Cloud Computing model<sup>2</sup> to reduce costs and improve services. Standards are critical to ensure cost-effective and easy migration, to ensure that mission-critical requirements can be met, and to reduce the risk that sizable investments may become prematurely technologically obsolete. Standards are key elements required to ensure a level playing field in the global marketplace.<sup>3</sup> The importance of setting standards in close relation with private sector involvement is highlighted in a memorandum from the White House: M-12-08,<sup>4</sup> dated January 17, 2012.

The NIST Cloud Computing Standards Roadmap Working Group has surveyed the existing standards landscape for interoperability, performance, portability, security, and accessibility standards/models/studies/use cases/conformity assessment programs, etc., relevant to cloud computing. Where possible, new and emerging standardization work has also been tracked and surveyed. Using this available information, current standards, standards gaps, and standardization priorities are identified within this document.

---

<sup>1</sup> This effort is consistent with the NIST role per the National Technology Transfer and Advancement Act (NTTAA) of 1995, which became law in March 1996.

<sup>2</sup> *NIST Definition of Cloud Computing*, Special Publication 800-145, "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

<sup>3</sup> This edition of the standards roadmap focuses on USG cloud computing requirements for interoperability, performance, portability, security, and accessibility, and does not preclude the needs to address other essential requirements.

<sup>4</sup> *Principles for Federal Engagement in Standards Activities to Address National Priorities*, January 17, 2012  
<http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-08.pdf>

The NIST Definition of Cloud Computing identified cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

As an extension to the above NIST cloud computing definition, a NIST cloud computing reference architecture has been developed by the NIST Cloud Computing Reference Architecture and Taxonomy Working Group that depicts a generic high-level conceptual model for discussing the requirements, structures and operations of cloud computing. It contains a set of views and descriptions that are the basis for discussing the characteristics, uses, and standards for cloud computing, and relates to a companion cloud computing taxonomy.<sup>5</sup>

Cloud computing use cases describe the consumer requirements when using cloud computing service offerings. Through its working groups as described below, the NIST Cloud Computing program has studied a range of U.S. federal government and general-purpose use cases to extract features that are amenable to standardization. Using these examples, the current document analyzes how existing cloud-related standards fit the needs of federal cloud consumers and identifies standardization gaps.

Cloud computing standards are already available in support of many of the functions and requirements. 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. Other standards have been developed or are now being developed to support specific cloud computing functions and requirements, such as virtualization, infrastructure management, service level agreements (SLAs), audits and cloud-specific data handling. Wherever possible, applicable standards are identified in this document.

To assess the state of standardization in support of cloud computing, the NIST Cloud Computing Standards Roadmap Working Group has compiled an [Inventory of Standards Relevant to Cloud Computing](#).<sup>6</sup> This inventory is being maintained and updated as necessary. Using the taxonomy developed by the NIST Cloud Computing Reference Architecture and Taxonomy Working Group, cloud computing relevant standards have been mapped to the requirements of accessibility, interoperability, performance, portability, and security.

---

<sup>5</sup> NIST Special Publication 500-292, *NIST Cloud Computing Reference Architecture*, September 2011  
[http://www.nist.gov/customcf/get\\_pdf.cfm?pub\\_id=909505](http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505)

<sup>6</sup> <http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/StandardsInventory>

Present areas with standardization gaps include: SaaS (Software as a Service) functional interfaces; SaaS self-service management interfaces; PaaS (Platform as a Service) functional interfaces; business support / provisioning / configuration; security; and privacy. Present standardization areas of priority to the federal government include: security auditing and compliance; identity and access management; SaaS application specific data and metadata; and resource description and discovery.

While there are only a few approved cloud computing specific standards at present, there is a fast-changing landscape of cloud computing-relevant standardization under way in a number of Standards Developing Organizations (SDOs). Every effort has been made in the context of the NIST Cloud Computing Standards Roadmap to engage with and to gather input from SDOs active in this area. Federal agencies should also be encouraged to participate specifically in cloud computing standards development projects that support the specific needs and priorities of their cloud computing services. Specific recommendations regarding engagement between federal agencies and SDOs are:

### **Recommendation 1 – Contribute Agency Requirements**

Agencies should coordinate and contribute clear and comprehensive user requirements for cloud computing standards projects.

### **Recommendation 2 – Participate in Standards Development**

Agencies should actively participate and coordinate in cloud computing standards development projects that are of high priority to their agency missions. The January 17, 2012, White House Memorandum, M-12-08,<sup>7</sup> lists five fundamental strategic objectives for federal government agencies whenever engaging in standards development.

### **Recommendation 3 – Encourage Testing to Accelerate Technically Sound Standards-Based Deployments**

Agencies should support the concurrent development of conformity and interoperability assessment schemes to accelerate the development and use of technically sound cloud computing standards and standards-based products, processes, and services. Agencies should also include consideration of conformity assessment approaches currently in place that take account of elements from international systems, to minimize duplicative testing and encourage private sector support.

---

<sup>7</sup> [Principles for Federal Engagement in Standards Activities to Address National Priorities](#), January 17, 2012

**Recommendation 4 – Specify Cloud Computing Standards**

Agencies should specify cloud computing standards in their procurements and grant guidance when multiple vendors offer standards-based implementations and there is evidence of successful interoperability testing.

**Recommendation 5 – USG-Wide Use of Cloud Computing Standards**

To support USG requirements for accessibility, interoperability, performance, portability, and security in cloud computing, the Federal Cloud Computing Standards and Technology Working Group, in coordination with the Federal CIO Council Cloud Computing Executive Steering Committee (CCESC) and the Cloud First Task Force, should recommend specific cloud computing standards and best practices for USG-wide use.

## 2 INTRODUCTION

### 2.1 BACKGROUND

U.S. laws and associated policy require federal agencies to use international, voluntary consensus standards in their procurement and regulatory activities, except where inconsistent with law or otherwise impractical.

The National Institute of Standards and Technology (NIST) has been designated by the Federal Chief Information Officer (CIO) to accelerate the federal government's secure adoption of cloud computing by leading efforts to identify existing standards and guidelines. Where standards are needed, NIST works closely with U.S. industry, standards developers, other government agencies, and leaders in the global standards community to develop standards that will support secure cloud computing.

The NIST Cloud Computing Program was formally launched in November 2010 and was created to support the federal government effort to incorporate cloud computing as a replacement for, or enhancement to, traditional information system and application models where appropriate.

The NIST Cloud Computing Program operates in coordination with other federal cloud computing implementation efforts (CIO Council/Information Security and Identity Management Committee [ISIMC], etc.) and is integrated with the Federal CIO's 25-point IT Implementation Plan for the federal government.

At the beginning of 2011, NIST created the following public working groups in order to provide a technically oriented strategy and standards-based guidance for the federal cloud computing implementation effort:

- Cloud Computing Reference Architecture and Taxonomy Working Group
- Cloud Computing Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC) Working Group
- Cloud Computing Security Working Group
- Cloud Computing Standards Roadmap Working Group
- Cloud Computing Target Business Use Cases Working Group

## 2.2 NIST CLOUD COMPUTING VISION

NIST seeks to provide leadership and guidance around the cloud computing paradigm to catalyze its use within industry and government. NIST also strives to shorten the adoption life cycle, which will enable near-term cost savings and increased ability to quickly create and deploy safe and secure enterprise solutions. Furthermore, NIST is committed to foster cloud computing practices that support interoperability, portability, and security requirements that are appropriate and achievable for various usage scenarios, by focusing on the necessary standards, specifications, and guidance that must be in place for these requirements to be met.<sup>8</sup>

The NIST area of focus is technology, and specifically, interoperability, portability, and security requirements, standards, and guidance. In this version of the document, accessibility and performance have also been included. The intent is to use the standards strategy to prioritize NIST tactical projects which support USG agencies in the secure and effective adoption of the cloud computing model to support their missions. The expectation is that these priorities will benefit industry, SDOs, cloud adopters, and policy makers.

In this document, privacy as a standards issue is narrowly dealt with under confidentiality, a subset of information security. Confidentiality includes preserving authorized restrictions on access and disclosure, including means for protecting personal privacy. Because privacy requirements are mostly policy decisions, they are often developed by governments as laws and not by SDOs. Appendix J of [NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations](#), includes a catalog of privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations, organizational assets, individuals, other organizations, etc., from a diverse set of threats including hostile cyber-attacks, natural disasters, structural failures, and human errors (both intentional and unintentional).

---

<sup>8</sup> SP 500-293 Volume II, US Government Cloud Computing Technology Roadmap Volume II (Draft) Release 1.0  
[http://www.nist.gov/itl/cloud/upload/SP\\_500\\_293\\_volumeII.pdf](http://www.nist.gov/itl/cloud/upload/SP_500_293_volumeII.pdf)

### 2.3 NIST CLOUD COMPUTING STANDARDS ROADMAP WORKING GROUP

SDOs and others have and are developing supporting cloud computing documents to include standards, conceptual models, reference architectures, conformity assessment programs, and standards roadmaps to facilitate communication, data exchange, and security for cloud computing and its application. Still other standards are emerging to focus on technologies that support cloud computing, such as virtualization. The NIST Cloud Computing Standards Roadmap Working Group is leveraging this existing, publicly available work, plus the work of the other NIST working groups, to develop a NIST Cloud Computing Standards Roadmap that can be incorporated into the NIST USG Cloud Computing Technology Roadmap.

### 2.4 HOW THIS REPORT WAS PRODUCED

The NIST Cloud Computing Standards Roadmap Working Group (CCSRWG) has surveyed the existing standards landscape for interoperability, performance, portability, security, and accessibility standards / models / studies / use cases / conformity assessment programs, etc., relevant to cloud computing. Using this available information, standards, standards gaps or overlaps, and standardization priorities have been identified, thereby providing a clearer picture of this evolving technical landscape.

### 3 THE NIST DEFINITION OF CLOUD COMPUTING<sup>9</sup>

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

#### 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 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 elastically provisioned and released, 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<sup>10</sup> at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, active user accounts). Resource usage can be monitored, controlled, audited, and reported, providing transparency for both the provider and consumer of the utilized service.

---

<sup>9</sup> NIST Special Publication 800-145, *NIST Definition of Cloud Computing*, September 2011

<sup>10</sup> Typically this is done on a pay-per-use or charge-per-use basis.

## Service Models:

*Software as a Service (SaaS).* The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure.<sup>11</sup> The applications are accessible from various client devices through either 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.

*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, libraries, services, and tools supported by the provider.<sup>12</sup> 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 configuration settings for the application-hosting environment.

*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, and deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

## 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.

---

<sup>11</sup> A 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, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.

<sup>12</sup> This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.

*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).

## 4 CLOUD COMPUTING REFERENCE ARCHITECTURE<sup>13</sup>

The NIST cloud computing definition is widely accepted and valuable in providing a clear understanding of cloud computing technologies and cloud services. The NIST cloud computing reference architecture presented in this section is a natural extension to the NIST cloud computing definition.

The NIST cloud computing reference architecture is a generic high-level conceptual model that is a powerful tool for discussing the requirements, structures, and operations of cloud computing. The model is not tied to any specific vendor products, services, or reference implementation, nor does it define prescriptive solutions that inhibit innovation. It defines a set of actors, activities, and functions that can be used in the process of developing cloud computing architectures, and relates to a companion cloud computing taxonomy. It contains a set of views and descriptions that are the basis for discussing the characteristics, uses, and standards for cloud computing.

The NIST cloud computing reference architecture focuses on the requirements of what cloud service provides, not on a design that defines a solution and its implementation. It is intended to facilitate the understanding of the operational intricacies in cloud computing. The reference architecture does not represent the system architecture of a specific cloud computing system; instead, it is a tool for describing, discussing, and developing the system-specific architecture using a common framework of reference.

The design of the NIST cloud computing reference architecture serves the objectives to: illustrate and understand various cloud services in the context of an overall cloud computing conceptual model; provide technical references to USG agencies and other consumers to understand, discuss, categorize, and compare cloud services; and communicate and analyze security, interoperability, and portability candidate standards and reference implementations.

### 4.1 OVERVIEW

The Overview of the Reference Architecture describes five major actors with their roles and responsibilities using the newly developing Cloud Computing Taxonomy. The NIST cloud computing reference architecture defines five major actors: cloud consumer, cloud provider, cloud auditor, cloud broker, and cloud carrier (See Figure 1: Cloud Actors). These core individuals have key roles in the realm of cloud computing. Each actor is an entity (a person or an organization) that participates in a transaction or process and/or performs tasks in cloud computing. For example, a Cloud Consumer is an individual or organization that acquires and uses cloud products and services. The purveyor of products and services is the Cloud Provider. Because of the possible service

---

<sup>13</sup> NIST Special Publication 500-292, *NIST Cloud Computing Reference Architecture*, September 2011

offerings (Software, Platform or Infrastructure) allowed for by the cloud provider, there will be a shift in the level of responsibilities for some aspects of the scope of control, security and configuration. The Cloud Broker acts as the intermediary between consumer and provider and will help consumers through the complexity of cloud service offerings and may also create value-added cloud services. The Cloud Auditor provides a valuable inherent function for the government by conducting the independent performance and security monitoring of cloud services. The Cloud Carrier is the organization which has the responsibility of transferring the data, somewhat akin to the power distributor for the electric grid.

Figure 1 – **Cloud Actors** briefly lists the five major actors defined in the NIST cloud computing reference architecture.

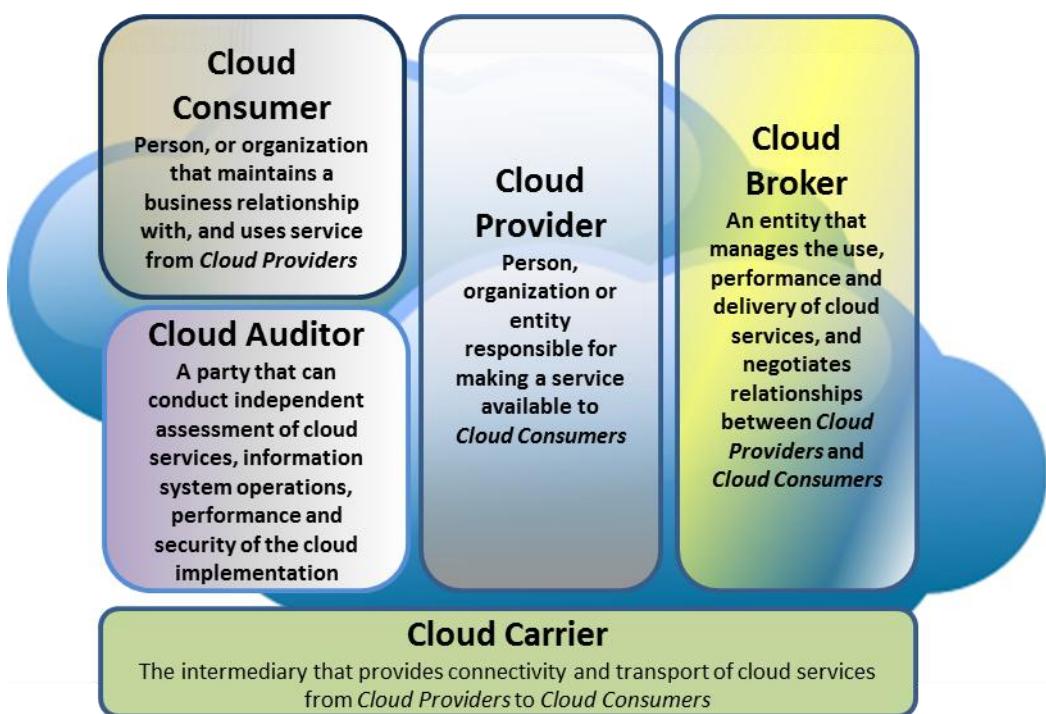
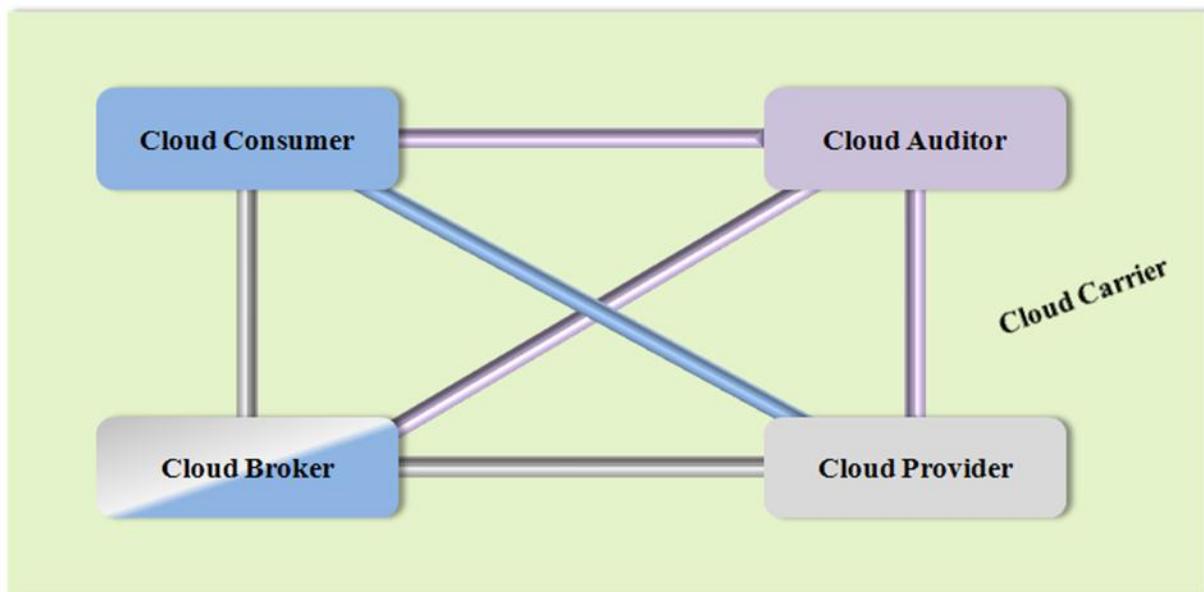


Figure 1 – Cloud Actors

Figure 2 – Interactions between the Actors in Cloud Computing shows the interactions among the actors in the NIST cloud computing reference architecture. A cloud consumer may request cloud services from a cloud provider directly or via a cloud broker. A cloud auditor conducts independent audits and may contact the others to collect necessary information. The details will be discussed in the following sections and be presented as successive diagrams in increasing levels of detail.



- The communication path between a cloud provider and a cloud consumer
- The communication paths for a cloud auditor to collect auditing information
- The communication paths for a cloud broker to provide service to a cloud consumer

Figure 2 – Interactions between the Actors in Cloud Computing

#### 4.2 CLOUD CONSUMER

The cloud consumer is the ultimate stakeholder that the cloud computing service is created to support. A cloud consumer represents a person or organization that maintains a business relationship with, and uses the service from, a cloud provider. A cloud consumer browses the service catalog from a cloud provider, requests the appropriate service, sets up service contracts with the cloud provider, and uses the service. The cloud consumer may be billed for the service provisioned, and needs to arrange payments accordingly. Depending on the services requested, the activities and usage scenarios can be different among cloud consumers, as shown in Table 1. Some example usage scenarios are listed in Figure 3.

Service Models	Consumer Activities	Provider Activities
SaaS	Uses application/service for business process operations.	Installs, manages, maintains, and supports the software application on a cloud infrastructure.
PaaS	Develops, tests, deploys, and manages applications hosted in a cloud system.	Provisions and manages cloud infrastructure and middleware for the platform consumers; provides development, deployment, and administration tools to platform consumers.
IaaS	Creates/install, manages, and monitors services for IT infrastructure operations.	Provisions and manages the physical processing, storage, networking, and the hosting environment and cloud infrastructure for IaaS consumers.

Table 1 – Cloud Consumer and Cloud Provider

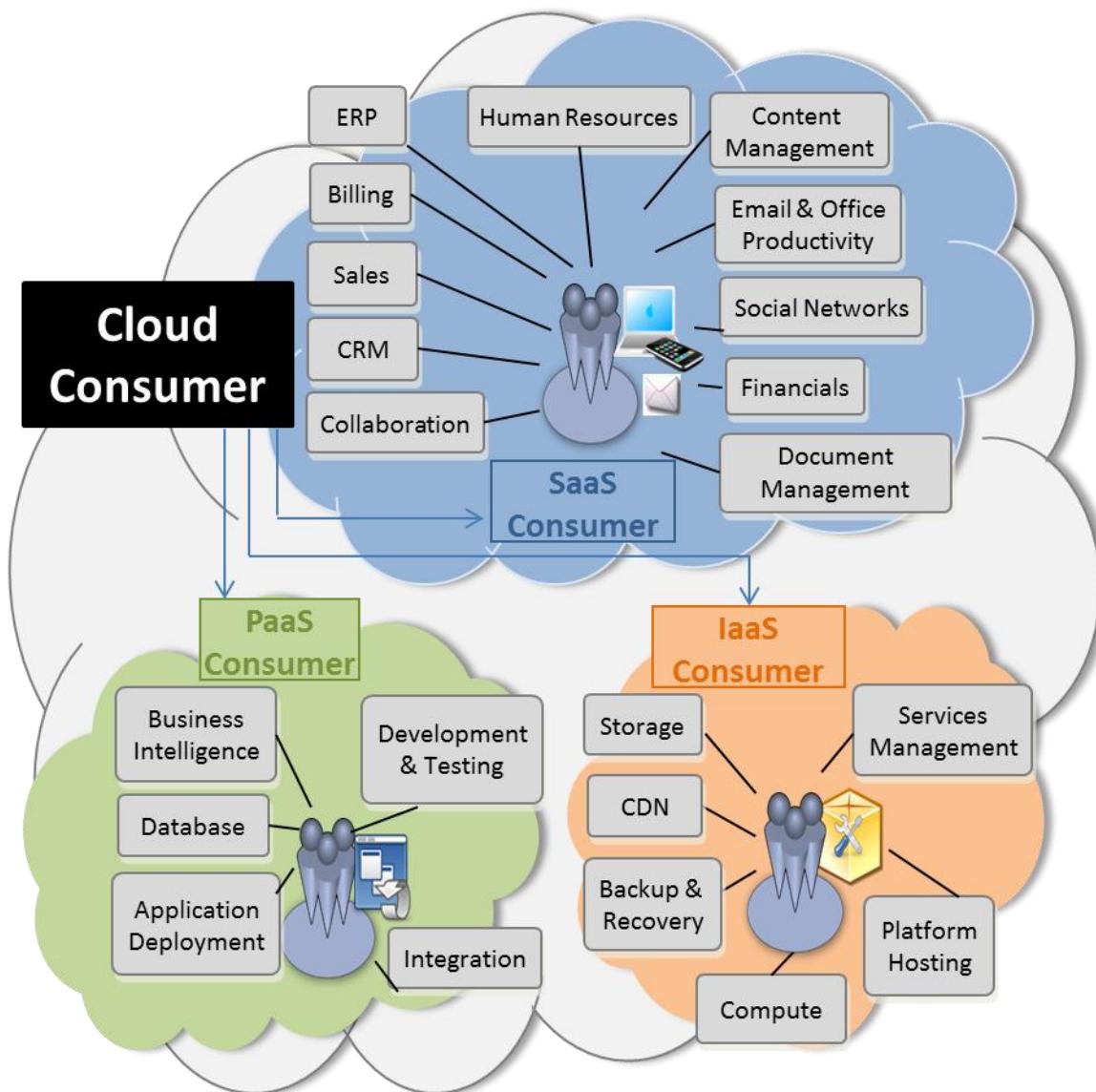


Figure 3 – Example of Services Available to a Cloud Consumer

SaaS applications are usually deployed as hosted services and are accessed via a network connecting SaaS consumers and providers. The SaaS consumers can be organizations that provide their members with access to software applications, end users who directly use software applications, or software application administrators who configure applications for end users. SaaS consumers access and use applications on demand, and can be billed on the number of consumers or the amount of consumed services. The latter can be measured in terms of the time in use, the network bandwidth consumed, or the amount/duration of data stored.

For PaaS, cloud consumers employ the tools and execution resources provided by cloud providers for the purpose of developing, testing, deploying, and managing applications hosted in a cloud system. PaaS consumers can be application developers who design and implement application software, application testers who run and test applications in various cloud systems, application deployers who publish applications into a cloud system, and application administrators who configure and monitor application performance on a platform. PaaS consumers can be billed by the number of consumers, the type of resources consumed by the platform, or the duration of platform usage.

For IaaS, consumers are provisioned with the capabilities to access virtual computers, network-accessible storage, network infrastructure components, and other fundamental computing resources, on which consumers can deploy and run arbitrary software. IaaS consumers can be system developers, system administrators, and information technology (IT) managers who are interested in creating, installing, managing and monitoring services for IT infrastructure operations. IaaS consumers are provisioned with the capabilities to access these computing resources, and are billed for the amount of resources consumed.

#### 4.3 CLOUD PROVIDER

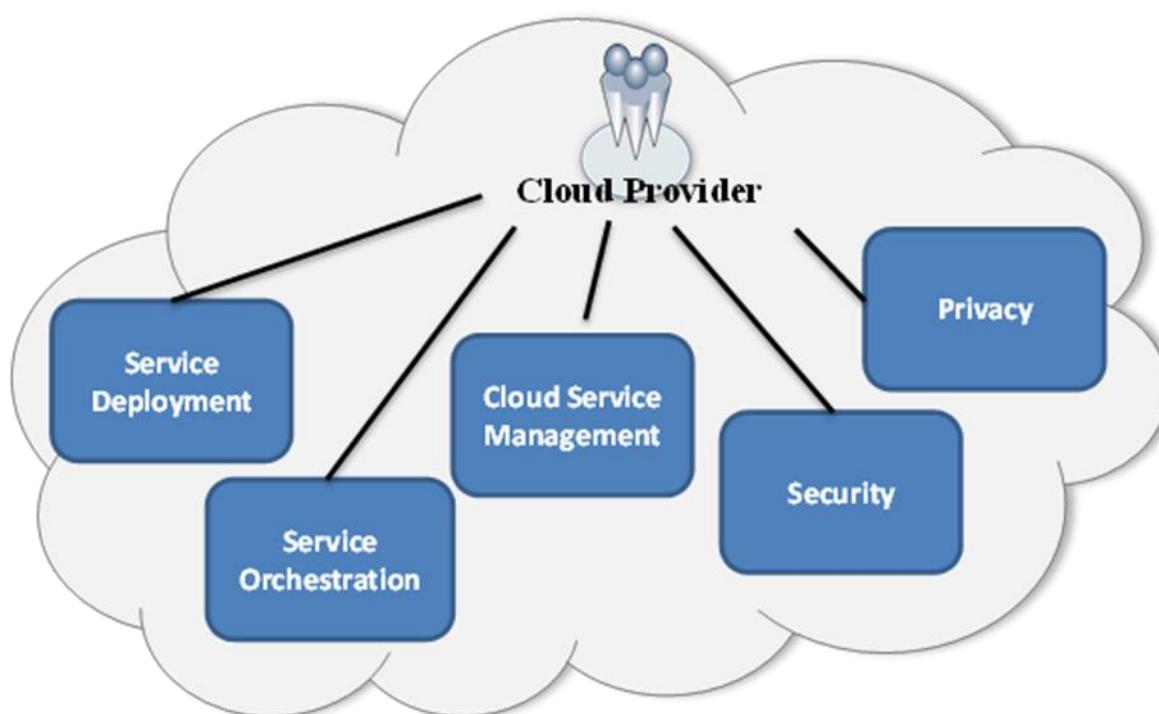


Figure 4 – Cloud Provider: Major Activities

A cloud provider can be a person, an organization, or an entity responsible for making a service available to cloud consumers. A cloud provider builds the requested software/platform/infrastructure services, manages the technical infrastructure required for providing the services, provisions the services at agreed-upon service levels, and protects the security and privacy of the services. As illustrated in Figure 4 – Cloud Provider: Major Activities, cloud providers undertake different tasks for the provisioning of the various service models.

For SaaS, the cloud provider deploys, configures, maintains, and updates the operation of the software applications on a cloud infrastructure so that the services are provisioned at the expected service levels to cloud consumers. The provider of SaaS assumes most of the responsibilities in managing and controlling the applications and the infrastructure, while the cloud consumers have limited administrative control of the applications.

For PaaS, the cloud provider manages the cloud infrastructure for the platform, and provisions tools and execution resources for the platform consumers to develop, test, deploy, and administer applications. Consumers have control over the applications and possibly the hosting environment settings, but cannot access the infrastructure underlying the platform including network, servers, operating systems, or storage.

For IaaS, the cloud provider provisions the physical processing, storage, networking, and other fundamental computing resources, as well as manages the hosting environment and cloud infrastructure for IaaS consumers. Cloud consumers deploy and run applications, have more control over the hosting environment and operating systems, but do not manage or control the underlying cloud infrastructure (e.g., the physical servers, network, storage, hypervisors, etc.).

The activities of cloud providers can be discussed in greater detail from the perspectives of *Service Deployment, Service Orchestration, Cloud Service Management, Security and Privacy*.

#### 4.3.1 SERVICE DEPLOYMENT

As identified in the NIST cloud computing definition, a cloud infrastructure may be operated in one of the following deployment models: *public cloud, private cloud, community cloud, or hybrid cloud*. For the details related to the controls and management in the cloud, we refer readers to the NIST Special Publication 800-146, *NIST Cloud Computing Synopsis and Recommendations*.

A public cloud is one in which the cloud infrastructure and computing resources are made available to the general public over a public network. A public cloud is owned by an organization selling cloud services and serves a diverse pool of clients.

For private clouds, the cloud infrastructure is operated exclusively for a single organization. A private cloud gives the organization exclusive access to and usage of the infrastructure and computational resources. It may be managed either by the organization or by a third party, and may

be implemented at the organization's premise (i.e., *on-site private clouds*) or outsourced to a hosting company (i.e., *outsourced private clouds*).

Similar to private clouds, a community cloud may be managed by the organizations or by a third party, and may be implemented at the customer's location (i.e., *on-site community cloud*) or outsourced to a hosting company (i.e., *outsourced community cloud*). However, a community cloud serves a set of organizations that have common security, privacy, and compliance considerations, rather than serving a single organization as does a private cloud.

A hybrid cloud is a composition of two or more cloud deployment models (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability. As discussed in this section, both private clouds and community clouds can be either implemented on-site or outsourced to a third party. Therefore, each constituent cloud of a hybrid cloud can be one of the five variants.

#### 4.3.2 SERVICE ORCHESTRATION

Service orchestration refers to the arrangement, coordination, and management of cloud infrastructure to provide the optimizing capabilities of cloud services, as a cost-effective way of managing IT resources, as dictated by strategic business requirements. Figure 5 shows the general requirements and processes for cloud providers to build each of the three service models.

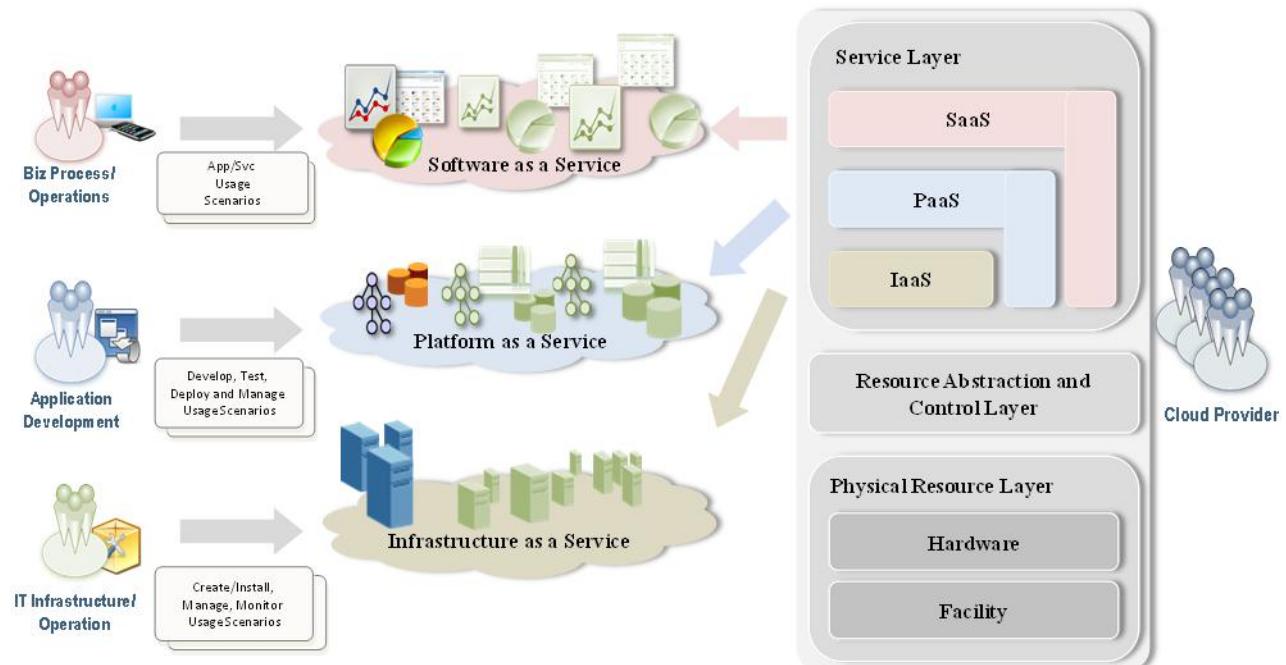


Figure 5 – Cloud Provider: Service Orchestration

A three-layered framework is identified for a generalized cloud system in Figure 5. The top layer is the service layer, where a cloud provider defines and provisions each of the three service models. This is where cloud consumers consume cloud services through the respective cloud interfaces.

The middle layer is the resource abstraction and control layer. This layer contains the system components that a cloud provider uses to provide and manage access to the physical computing resources through software abstraction. The layer typically includes software elements such as hypervisors, virtual machines, virtual data storage, and other resource abstraction and management components needed to ensure efficient, secure, and reliable usage. While virtual machine technology is commonly used at this layer, other means of providing the necessary software abstractions are not precluded. This layer provides “cloud readiness” with the five characteristics defined in the NIST definition of cloud computing.

The lowest layer in the framework is the physical resource layer, which includes all the physical computing resources. This layer includes hardware resources, such as computers (CPU and memory), networks (routers, firewalls, switches, network links, and interfaces), storage components (hard disks), and other physical computing infrastructure elements. It also includes facilities resources, such as heating, ventilation, and air conditioning (HVAC), power, communications, and other aspects of the physical plant.

Note that in this framework, the horizontal positioning of layers implies a stack in which the upper layer has a dependency on the lower layer. The resource abstraction and control layer build virtual cloud resources on top of the underlying physical resource layer and support the service layer where cloud services interfaces are exposed. The three service models can be built either on top of one another (i.e., SaaS built upon PaaS and PaaS built upon IaaS) or directly upon the underlying cloud infrastructure. For example, a SaaS application can be implemented and hosted on virtual machines from IaaS or directly on top of cloud resources without using IaaS.

#### 4.3.3 CLOUD SERVICE MANAGEMENT

*Cloud Service Management* includes all of the service-related functions that are necessary for the management and operation of those services required by or proposed to cloud consumers. As illustrated in Figure 6, cloud service management can be described from the perspective of *business support, provisioning and configuration, and from the perspective of portability and interoperability requirements*.

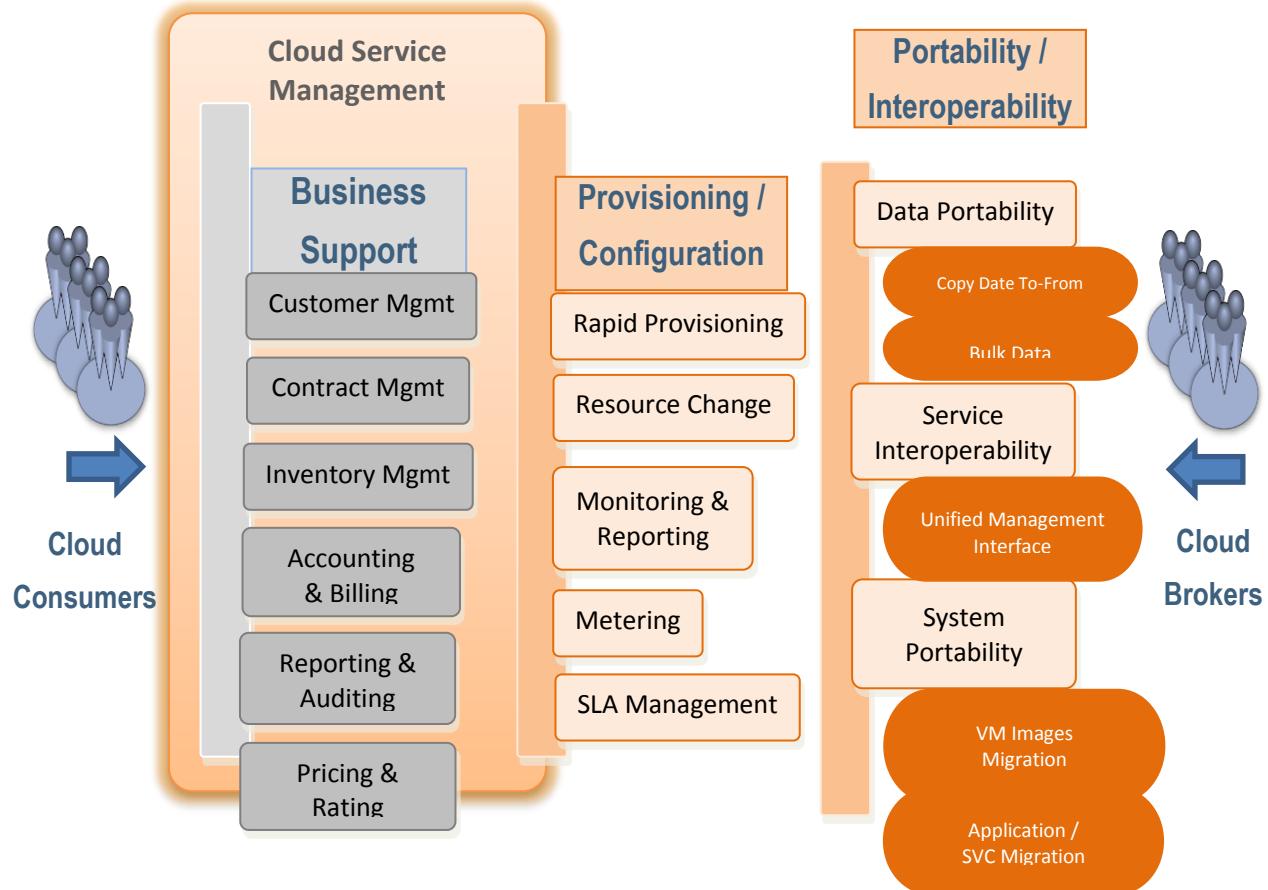


Figure 6 – Cloud Provider: Cloud Service Management

#### 4.3.4 SECURITY

“As the Federal Government moves to the cloud, it must be vigilant to ensure the security and proper management of government information to protect the privacy of citizens and national security” (by Vivek Kundra, Federal Cloud Computing Strategy, February 2011.) In July 2012, the U.S. Department of Defense released a Cloud Computing Strategy, which stated “the Department has specific cloud computing challenges that require careful adoption considerations, especially in areas of cybersecurity, continuity of operations, information assurance (IA), and resilience.” Also, in November 2012, NIST published a White Paper – *Challenging Security Requirements for U.S. Government Cloud Computing Adoption*. This document provides an overview of the high-priority security challenges perceived by federal agencies as impediments to the adoption of cloud computing.

Security is a cross-cutting function that spans all layers of the reference architecture (see Figure 12 – The Combined Conceptual Reference Diagram), involving end-to-end security that ranges from physical security to application security, and in general, the responsibility is shared between cloud provider and federal cloud consumer. For example, the protection of the physical resource layer (see Figure 5 – Cloud Provider: Service Orchestration) requires physical security that denies unauthorized access to the building, facility, resource, or stored information. Cloud Providers should ensure that the facility hosting cloud services is secure and that the staff has proper background checks. When data or applications are moved to a cloud, Cloud Consumers ensure that the cloud offering satisfies the security requirements and enforces the compliance rules. Several U.S. government agencies provide computer security guidance, and that the cloud system should support the most up-to-date guidance. It is also important to note that security, compliance, and policy requirements are a function of the legal jurisdiction of the country in which the cloud services are provided and can vary from country to country. An independent audit (see Section 3.4) should be conducted to verify the compliance with regulations or security policies.

#### 4.3.5 PRIVACY

Cloud providers should protect the assured, proper, and consistent collection, processing, communication, use, and disposition of personal information (PI) and personally identifiable information (PII) in the cloud system. PII is the information that can be used to distinguish or trace an individual's identity, such as name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. The CIO Council – [Privacy Committee](#)<sup>14</sup> has identified privacy and protection of collected PII as one of the federal government key business imperatives. Though cloud computing provides a flexible solution for shared resources, software, and information, it also poses additional privacy challenges to consumers using the clouds.

The Digital Government Strategy<sup>15</sup> issued by the Federal Chief Information Officer (CIO) on May 23, 2012 sets forth a new vision of how government is to connect with and provide services to the American people, harnessing the power of digital technology and enabling citizens and the federal workforce to securely access government digital information, data, and services anywhere, and

---

<sup>14</sup> <https://cio.gov/about/committees/privacy-committee/>

<sup>15</sup> *Digital Government: Building a 21<sup>st</sup> Century Platform to Better Serve the American People* (May 23, 2012), (Strategy) <http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html>

anytime (Recommendations).<sup>16</sup> The Federal CIO Council released *Recommendations for Standardized Implementation of Digital Privacy Controls* (Recommendations), which discusses three fundamental privacy controls: PII Inventory, Privacy Impact Assessment (PIA), and Privacy Notice. The Recommendations are that agencies identify and consider all PII that may be collected or otherwise exposed through a particular digital technology, analyze the privacy risks through the data life cycle by conducting and updating a PIA (as needed), and provide notice to individuals of when and how their PII will be collected, used, retained, and disclosed.

Furthermore, federal agencies should be aware of the privacy concerns associated with the cloud computing environment where data are stored on a server that is not owned or controlled by the federal government. Privacy impact assessment (PIA) can be conducted, as needed, to measure how well the cloud system conforms to applicable legal, regulatory, and policy requirements regarding privacy. A PIA can help federal agencies comply with applicable privacy laws and regulations governing an individual's privacy, and to ensure confidentiality, integrity, and availability of an individual's personal information at every stage of development and operation.

In furthering the milestone action goal of the Digital Government Strategy for addressing digital privacy, records retention, and security issues, the National Archives & Records Administration (NARA) has issued Electronic Records Management (ERM) guidance for digital content created, collected, or maintained by federal agencies<sup>17</sup>. NARA also serves as managing partner of the E-Government ERM Initiative, coordinating the development and issuance of enterprise-wide ERM tools and electronic information standards, to support the interoperability of federal agency record systems and improve customer service (e.g., digital records access).<sup>18</sup>

---

<sup>16</sup> *Recommendations for Standardized Implementation of Digital Privacy Controls* (December 2012), [https://cio.gov/wp-content/uploads/downloads/2012/12/Standardized\\_Digital\\_Privacy\\_Controls.pdf](https://cio.gov/wp-content/uploads/downloads/2012/12/Standardized_Digital_Privacy_Controls.pdf)

<sup>17</sup> <http://www.archives.gov/records-mgmt/initiatives/erm-guidance.html>.

<sup>18</sup> <http://www.archives.gov/records-mgmt/initiatives/erm-overview.html>.

#### 4.4 CLOUD AUDITOR

A cloud auditor is a party that can conduct independent assessment of cloud services, information system operations, performance, and the security of a cloud computing implementation. A cloud auditor can evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance, and adherence to service level agreement parameters.

Auditing is especially important for federal agencies as “agencies should include a contractual section enabling third parties to assess security controls of cloud providers” (*by Vivek Kundra, Federal Cloud Computing Strategy, February 2011*). Security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information. For security auditing, a cloud auditor can make an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to the security requirements for the system. The security auditing should include the verification of the compliance with regulation and security policy.

#### 4.5 CLOUD BROKER

The NIST Reference Architecture, SP 500-292,<sup>19</sup> defines a Cloud Broker as an entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers. As cloud computing evolves, the integration of cloud services may become too complex for cloud Consumers to manage. In such cases, a Cloud Consumer may request cloud services from a Cloud Broker instead of directly contacting a Cloud Provider. Cloud Brokers provide a single point of entry for managing multiple cloud services. The key defining feature that distinguishes a Cloud Broker from a Cloud Service Provider is the ability to provide a single consistent interface to multiple differing providers, whether the interface is for business or technical purposes. In general, Cloud Brokers provide services in three categories:

**Intermediation:** A Cloud Broker enhances a given service by improving some specific capability and providing value-added services to cloud Consumers. The improvement can be managing access to cloud services, identity management, performance reporting, enhanced security, etc.

**Aggregation:** A Cloud Broker combines and integrates multiple services into one or more new services. The Broker provides data and service integration and ensures the secure data movement between the cloud Consumer and multiple cloud Providers.

---

<sup>19</sup> [http://www.cloudcredential.org/images/pdf\\_files/nist%20reference%20architecture.pdf](http://www.cloudcredential.org/images/pdf_files/nist%20reference%20architecture.pdf)

**Arbitrage:** Service arbitrage is similar to service aggregation except that the services being combined/consolidated are not fixed. Service arbitrage means a Broker has the flexibility to choose services from multiple service Providers.

A Cloud Broker may provide:

1. Business and relationship support services (business intermediation), and
2. Technical support service (aggregation, arbitrage, and technical intermediation), with a key focus on handling interoperability issues among multiple Providers.

#### 4.6 CLOUD CARRIER

A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers. Cloud carriers provide access to consumers through network, telecommunication, and other access devices. For example, cloud consumers can obtain cloud services through network access devices, such as computers, laptops, mobile phones, mobile Internet devices (MIDs), etc. The distribution of cloud services is normally provided by network and telecommunication carriers or a *transport agent*, where a transport agent refers to a business organization that provides physical transport of storage media such as high-capacity hard drives. Note that a cloud provider will set up service level agreements (SLAs)<sup>20</sup> with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers, and may require the cloud carrier to provide dedicated and encrypted connections between cloud consumers and cloud providers.

---

<sup>20</sup> SLAs are agreements under the umbrella of the overall cloud computing contract between a CSP and a cloud consumer. SLAs define acceptable service levels to be provided by the CSP to its customers in measurable terms. The ability of a CSP to perform at acceptable levels is consistent among SLAs, but the definition, measurement and enforcement of this performance varies widely among CSPs. A cloud consumer should ensure that CSP performance is clearly specified in all SLAs, and that all such agreements are fully incorporated, either by full text or by reference, into the CSP contract. [Source: *Creating Effective Cloud Computing Contracts for the Federal Government – Best Practices for Acquiring IT as a Service* <https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf>

## 5 CLOUD COMPUTING USE CASES

Cloud computing use cases describe the consumer goals and actions for using cloud computing service offerings. Analyzing business and technical cloud computing use cases and the applicable standards provides an intuitive, utility-centric perspective for identifying requirements for all actors in the use case. This section leverages the business and technical use case outputs from other NIST Cloud Computing Program Working Groups. Section 8 presents an analysis regarding whether existing cloud-related standards fulfill key aspects of the use case for USG cloud consumers and highlights where the gaps for standardizations exist.

### 5.1 BUSINESS USE CASES

The Target Business Use Case Working Group produced a template for documenting specific use cases. This template includes a section titled “Concept of Operations” in which “Current System” and “Desired Cloud Implementation” states are described. The template also gathers information about integration with other systems, security requirements, and both local and remote network access considerations. A set of business use cases was collected describing candidate USG agency cloud deployments. The stories captured in these business use cases help to identify business drivers behind the adoption of cloud computing in USG agencies, provide background information on the relevant usage context, and expose general agency consumer concerns and issues through specific scenarios.

These use cases thus helped to document key technical requirements for USG cloud-related standards in the areas of security, interoperability, and portability studied for the formulation of this roadmap. Efforts are now underway to document similar requirements with respect to other key considerations, such as accessibility and performance of federal cloud-based business systems and services.

The “Cloud First”<sup>21</sup> directive provided by the Federal CIO is a more general expansion of this analysis to multiple interacting current systems and cloud implementations. This expansion is intended to support evolving business processes as further cloud deployments are implemented.

---

<sup>21</sup> 25 Point Implementation Plan to Reform Federal Information Technology Management  
<http://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf>

## 5.2 TECHNICAL USE CASES

The SAJACC Working Group has analyzed the output of the Business Use Case group, along with other community-provided documents and inputs, and produced a set of detailed cloud computing technical use case scenarios. These technical use cases captured and describe in detail the requirements, inputs, outputs, and failure and success conditions of cloud operations. They provide descriptions of how users or groups of users, called “actors,” interact with one or more cloud computing resource systems to achieve specific goals, such as “how to copy data objects into a cloud,” or “instantiate a virtual machine within a specific security context.”

The mapping from the high-level business use cases to the SAJACC technical use cases allows a detailed understanding of ways in which the business operational stories of specific agency consumers identify specific technical requirements. Such requirements, as expressed in SAJACC technical use cases, are then well suited to demonstrate the applicability of cloud computing software or standards. For example, the business use case of an agency consumer’s move of its virtualized computing infrastructure to an IaaS cloud vendor identifies “*Virtual Machine (VM) control: manage virtual machine instance state*” as a technical requirement to be met.

The SAJACC group has gathered detailed examples from U.S. federal agencies and analyzed them in terms of these technical use case scenarios. The results from this effort, along with demonstrations presented to the SAJACC group meetings, have been used to elucidate applicability of standards and the presence of standardization gaps in this current document. The rest of this section drives through the high-level business use cases to the general technical requirements expressed and analyzes where cloud standards help address these requirements.

## 5.3 DEPLOYMENT SCENARIO PERSPECTIVE

The “Cloud First” business use case requires more complex interactions between USG agency cloud consumer and cloud providers. There are three generic scenarios from which interaction scenarios are derived, as shown in Figure 7.

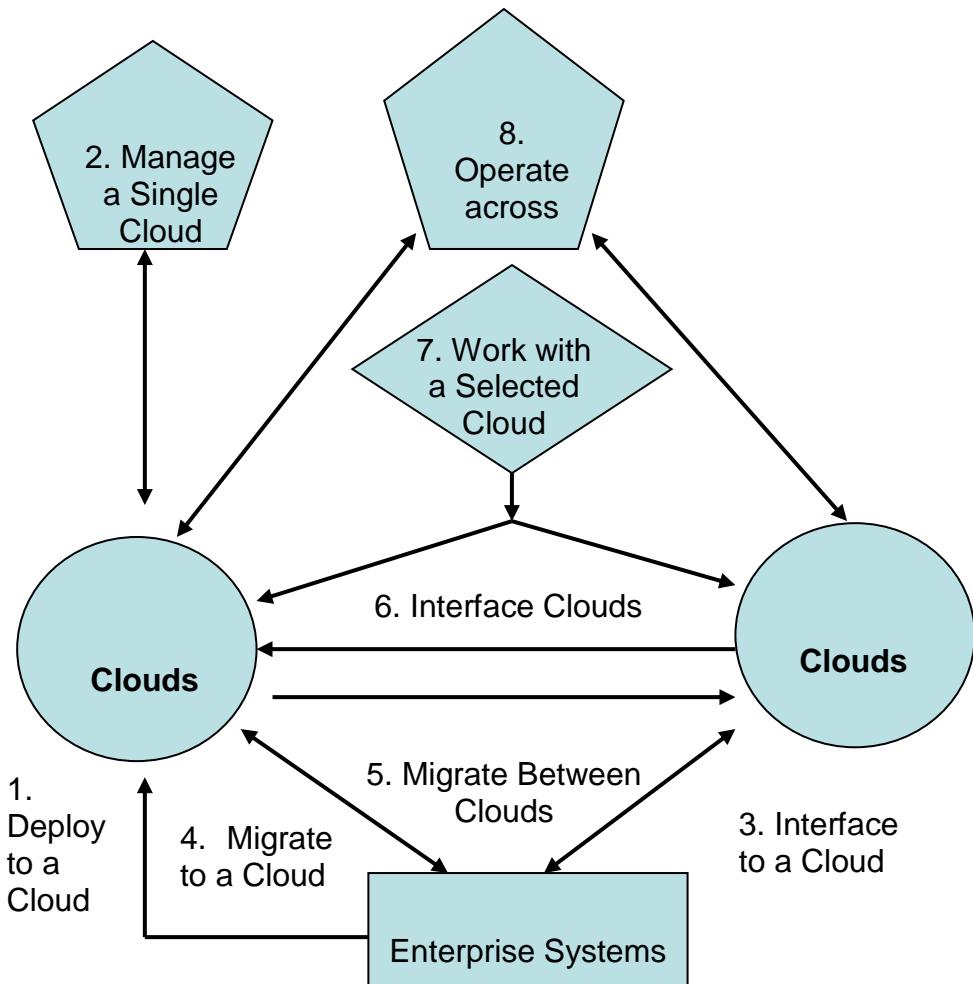


Figure 7 – High-Level Generic Scenarios

**Single Cloud System**

- Scenario 1: Deployment on a single cloud system
- Scenario 2: Manage resources on a single cloud system
- Scenario 3: Interface enterprise systems to a single cloud system
- Scenario 4: Enterprise systems migrated or replaced on a single cloud system

**Multiple Cloud Systems (serially, one at a time)**

- Scenario 5: Migration between cloud systems
- Scenario 6: Interface across multiple cloud systems
- Scenario 7: Work with a selected cloud system

**Multiple Cloud Systems** – (simultaneously, more than one at a time)

Scenario 8: Operate across multiple cloud systems

These technical use cases must also be analyzed in the context of their deployment models and the resultant way cloud actors must interact. These considerations identify two fundamental dimensions to the spectrum of cloud computing use cases:

- Centralized vs. Distributed, and
- Within vs. Crossing Trust Boundaries

These deployment cases will drive the requirements for cloud standards. They can be identified through the following matrix:

	a.) Within Trust Boundary	b.) Crossing Trust Boundary
1.) Centralized i.e., one administrative cloud domain	Deployment Case 1A	Deployment Case 1B
2.) Distributed, i.e., crossing administrative cloud domains	Deployment Case 2A	Deployment Case 2B

**Table 2 – Deployment Cases for High Level Scenarios**

Deployment Case 1: In the centralized deployment cases, there is one cloud provider under consideration at a time. Each cloud provider may service multiple cloud consumers. Each cloud consumer has a simple client-provider interaction with the provider.

Deployment Case 1A: This deployment case is typically a private cloud within a single administrative domain and trust boundary wherein policy and governance can be enforced by nontechnical means. Use cases within this deployment case may require standards to support the following basic technical requirements:

- Simple, consumer-provider authentication;
- VM management;
- Storage management;
- SLAs and performance/energy monitoring;
- Service discovery;
- Workflow management;

- Auditing; and
- Virtual organizations in support of community cloud use cases.

Deployment Case 1B: This deployment case is typically (commercial) public cloud within a single administrative domain but is outside of any trust boundary that a client could use to enforce policy and governance. Clients must rely on the cloud provider to enforce policy and governance through technical means that are "baked into" the infrastructure. Use cases within this deployment case may require standards to support the following additional technical requirements:

- SLAs in support of governance requirements, e.g., national or regional regulatory compliance;
- Stronger authentication mechanisms, e.g., Public Key Infrastructure (PKI) Certificates, etc.;
- Certification of VM isolation through hardware and hypervisor support;
- Certification of storage isolation through hardware support; and
- Data encryption.

Deployment Case 2: In the distributed deployment cases, a single cloud consumer has an application that may be distributed across two or more cloud providers and administrative domains simultaneously. While the cloud consumer may have simple consumer-provider interactions with their application and the providers, more complicated Peer-to-Peer ("P2P") interactions may be required -- between both the consumer and provider and also between the providers themselves.

Deployment Case 2A: This deployment case is typically a federated cloud of two or more administrative cloud domains, but where the cloud providers can agree "out of band" how to mutually enforce policy and governance -- essentially establishing a common trust boundary. Use cases within this deployment case may require standards to support the following basic technical requirements:

- P2P service discovery;
- P2P SLA and performance monitoring;
- P2P workflow management;
- P2P auditing;
- P2P security mechanisms for authentication, authorization; and
- P2P virtual organization management.

Deployment Case 2B: This deployment case is typically a hybrid cloud where applications cross a private-public trust boundary, or even span multiple public clouds, where both administrative domains and trust boundaries are crossed. Consumers must rely on the cloud provider to enforce policy and governance through technical means that are "baked into" the infrastructure. Applications and services may be distributed and need to operate in a P2P manner. Use cases within

this deployment case will require all the standards of the other deployment cases, in addition to the following more extensive technical requirements:

- P2P SLAs in support of governance requirements.

The use cases presented in this section will be analyzed with regards to their possible *deployment scenarios* to determine their requirements for standards. This analysis will subsequently be used to evaluate the likelihood of each of these deployment cases. Clearly the expected deployment of these use cases across the different deployment cases will not be uniform. This non-uniformity will assist in producing a *prioritized roadmap* for cloud standards. Likewise, in reviewing existing standards, these use cases – in conjunction with their possible deployment cases – will be used to identify and prioritize *gaps* in available standards.

Based on this analysis, note that Scenarios 1 through 4 could, in fact, be deployed on either a private cloud or a public cloud. Hence, the different standards noted in deployment cases 1A and 1B will be required. Scenarios 5, 6, and 7 (below) all involve the notion of the serial use of multiple clouds. Presumably these different clouds, used serially, could be either private or public. Hence, deployment cases 1A and 1B would also apply, but there are additional requirements to achieve portability, e.g., Application Programming Interface (API) commonality. Finally, Scenario 8 could involve a federated/community cloud or a hybrid cloud. Hence, deployment cases 2A and 2B would apply here.

To summarize the detailed technical use cases for this analysis, the following areas of technical requirements are common across all scenarios:

Scenarios	Technical Requirements
<b>1.</b>	Creating, accessing, updating, deleting data objects in cloud systems;
<b>2.</b>	Moving VMs and virtual appliances between cloud systems;
<b>3.</b>	Selecting the best IaaS vendor for private externally hosted cloud system;
<b>4.</b>	Tools for monitoring and managing multiple cloud systems;
<b>5.</b>	Migrating data between cloud systems;
<b>6.</b>	Single sign-on access to multiple cloud systems;
<b>7.</b>	Orchestrated processes across cloud systems;
<b>8.</b>	Discovering cloud resources;
<b>9.</b>	Evaluating SLAs and penalties; and
<b>10.</b>	Auditing cloud systems.

Table 3 – Scenarios and Technical Requirements

## 6 CLOUD COMPUTING STANDARDS

Standards are already available in support of many of the functions and requirements for cloud computing described in Section 3 and Section 4. 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. Other standards are now being developed in specific support of cloud computing functions and requirements, such as virtualization.

To assess the state of standardization in support of cloud computing, the NIST Cloud Computing Standards Roadmap Working Group has compiled an [Inventory of Standards Relevant to Cloud Computing](http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/StandardsInventory) <http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/StandardsInventory>.

### 6.1 INFORMATION AND COMMUNICATION TECHNOLOGIES (IT) STANDARDS LIFE CYCLE

Figure 8 is a high-level conceptualization of ways in which IT standards are developed and methods by which standards-based IT products, processes, and services are deployed. This figure is not meant to imply that these processes occur sequentially. Many of the processes illustrated can and should occur concurrently. Some of these processes (e.g., reference implementations, product / process / service / test tools development, testing, deployment) can and usually do also occur outside of the SDO process. These processes provide input and feedback to improve the standards, profiles, test tools, and associated stages of product development.

Cloud computing development has been characterized by its emergence during a period in which extremely interconnected and fast-moving product cycles have led to an explosion of innovation that strains the conventional SDO-based standards development process. While this is a rapidly changing area, cloud computing is not unique in this respect, and several other examples exist in history of similar periods of rapid change followed by standardization. In the long run, the processes that drive IT standards development are likely to follow historical precedent as over-arching requirements begin to become clear, and as standards emerge from such processes to fill these requirements. We therefore expect conformance testing, conformity assessment, and other processes related to the maturity and adoption of standards to emerge. Some evidence of this maturity is already starting to become manifest in the cloud standards landscape.

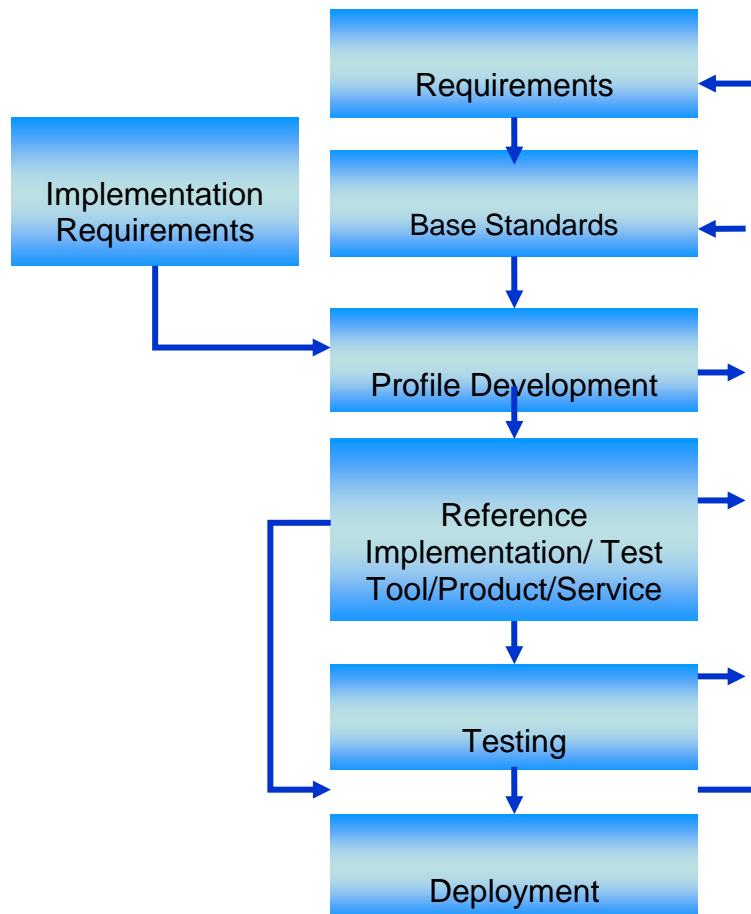


Figure 8 – IT Standards Life Cycle

## 6.2 THE ROLE OF CONFORMITY ASSESSMENT TO STANDARDS

Conformity assessment activities form a vital link between standards, which define necessary characteristics or requirements, and the products, services, and systems. Conformity assessment enables buyers, sellers, consumers, and regulators to have confidence that products, processes, and systems sourced in the global market meet specific requirements. It is the demonstration that specified requirements relating to a product, process, or system are fulfilled.

The characteristics of cloud computing including on-demand, self-service, and resource pooling among multiple tenants need to be considered when establishing conformance regimes for cloud services. For example, conformance testing may need to be done online against a production system that includes data and applications owned and controlled by other tenants. But privacy may preclude inspection of system logs, and it may not be possible to inspect the source code or run debugging tools. Test harnesses may not be able to be built into the service but may need to be run as a client

to the cloud service. It may be necessary to establish an account in order to access the service for testing.

#### 6.2.1 CONFORMITY ASSESSMENT ACTIVITIES

Conformity assessment procedures provide a means of ensuring that the products, services, systems, persons, or bodies have certain required characteristics, and that these characteristics are consistent from product to product, service to service, system to system, etc. Conformity assessment can include: supplier's declaration of conformity, sampling and testing, inspection, certification, management system assessment and registration, the accreditation of the competence of those activities, and recognition of an accreditation program's capability. A specific conformity assessment scheme or program may include one or more conformity assessment activities. While each of these activities is a distinct operation, they are closely interrelated.

Conformity assessment activities can be performed by many types of organizations or individuals. Conformity assessment can be conducted by: (1) a first party, which is generally the supplier or manufacturer; (2) a second party, which is generally the purchaser or user of the product; (3) a third party, which is an independent entity that is generally distinct from the first or second party and has no interest in transactions between the two parties; and (4) the government, which has a unique role in conformity assessment activities related to regulatory requirements.

Attestation consists of the issuance of a statement, based on a decision following review, that fulfillment of specified requirements has been demonstrated. First-party and third-party attestation activities are distinguished by the terms declaration (first party), certification (third party), and accreditation (third party).

A supplier's declaration of conformity is a first party (e.g., supplier) attestation that a product, process, service, etc., conforms to specified requirements. These requirements may include normative documents such as standards, guides, technical specifications, laws, and regulations. The supplier may conduct the testing or contract with a third party to do the testing. The test results are evaluated by the supplier, and when all requirements are met, the supplier issues a formal statement that the product is in conformance to the requirements. A statement that the product meets specific requirements can be included in the product documentation or other appropriate location, and the test results and other supporting documentation can be made available when requested.

Certification is a third-party attestation related to products, services, systems, etc. Accreditation is a third-party attestation related to a conformity assessment body conveying formal demonstration of its competence to carry out specific conformity assessment tasks. Testing laboratory accreditation provides formal recognition that a laboratory is competent to carry out specific tests or calibrations or types of tests or calibrations.

Rapidly advancing technology and increased international competition make it essential that suppliers have an opportunity to utilize all available options to minimize costs and ensure that the time to bring a product to market is at a minimum. Conformity assessment is an important aspect in

the development of product, processes and services, but this assessment does add costs and time to the development cycle.

---

#### 6.2.2 GOVERNMENT USE OF CONFORMITY ASSESSMENT SYSTEMS

Federal conformity-assessment activities are a means of providing confidence that the products, services, systems, etc. regulated or purchased by federal agencies, or that are the subject of federal assistance programs, have the required characteristics and/or perform in a specified manner. The NTTAA directs NIST to coordinate federal, state, and local government standards and conformity assessment activities with those of the private sector, with the goal of eliminating unnecessary duplication and complexity in the development and promulgation of conformity assessment requirements and measures. Conformity assessment that leverages existing private-sector programs can help lower the cost of implementation for agencies, and also provide added impetus for innovation and competitiveness. Numerous federal agencies are engaged in conformity assessment activities. In addition, as part of its role mandated by the NTTAA, many federal programs utilize NIST support to help design and implement appropriate and effective conformity assessment programs.

### 6.2.3 VISUALIZATION OF CONFORMITY ASSESSMENT PROCESSES

Figure 9 – Conformity Assessment Infrastructure provides an overview of the range of activities that can occur in conformity assessment and the relationships between them.

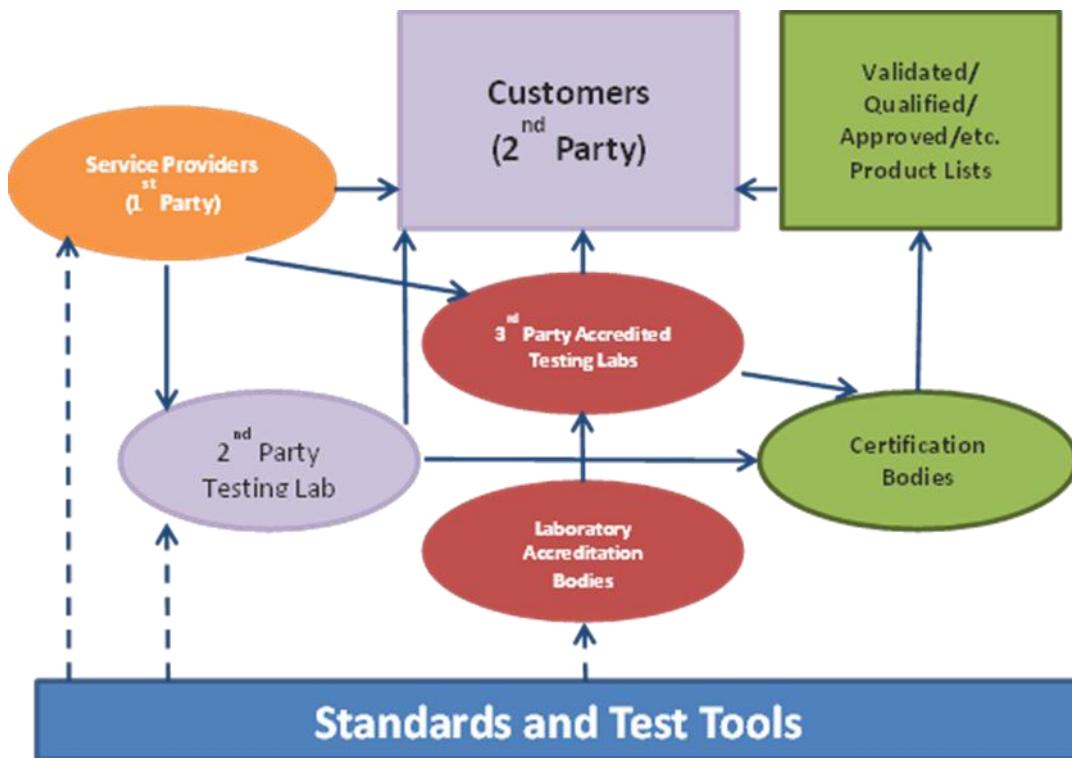


Figure 9 – Conformity Assessment Infrastructure

Figure 10 – Accreditation Process shows the relationships for the laboratory accreditation process. The key aspect of the process is the identification of the standards, test methods, test tools, and other technical requirements by the procurement agency as they apply to the products, services, systems, etc., to be tested.

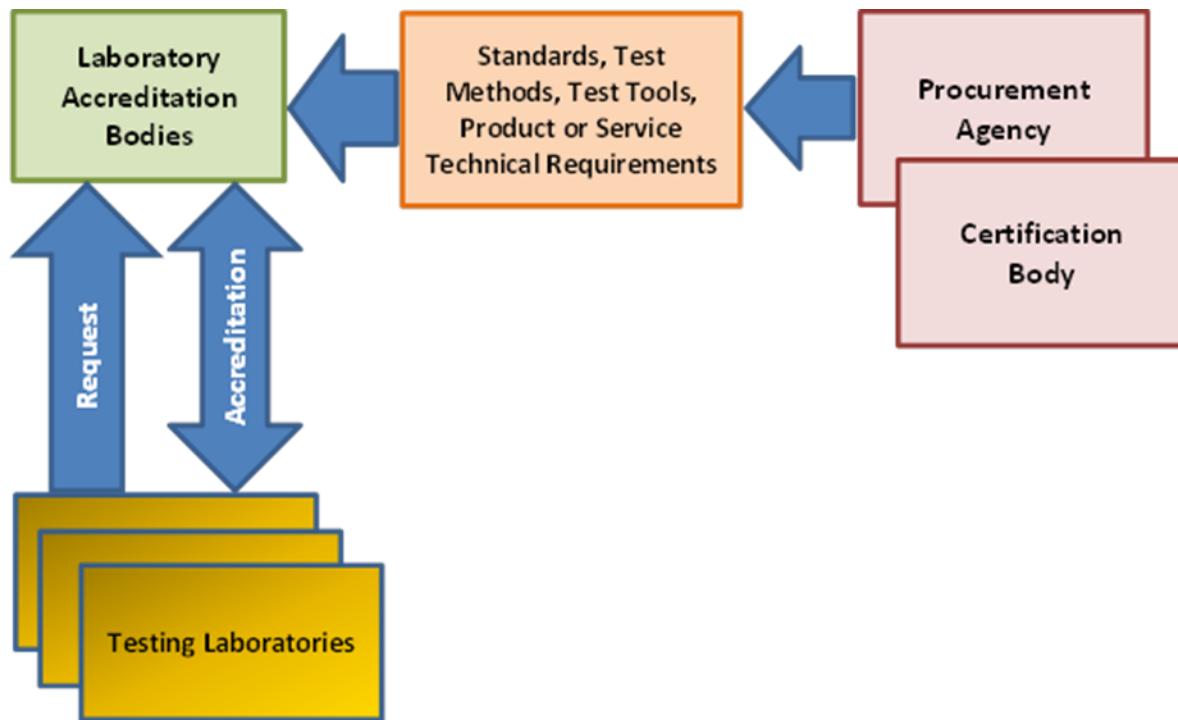


Figure 10 – Accreditation Process

An example of a conformity assessment system using accredited testing laboratories and certification is provided in Figure 11 – Assessment Process. The process starts with the submission by the supplier of the product, service, or system to a third-party accredited testing laboratory. The laboratory tests the product in accordance with the requirements and forwards the test results to the supplier. If the results are satisfactory to the supplier, they will be forwarded by the laboratory to the validation authority designated by the procurement agency in coordination with the qualified products list (QPL) owner. These experts will review the test reports and will make a recommendation as to their acceptance to the QPL owner. If the QPL owner agrees with the recommendations, the product, service, or system will be listed.

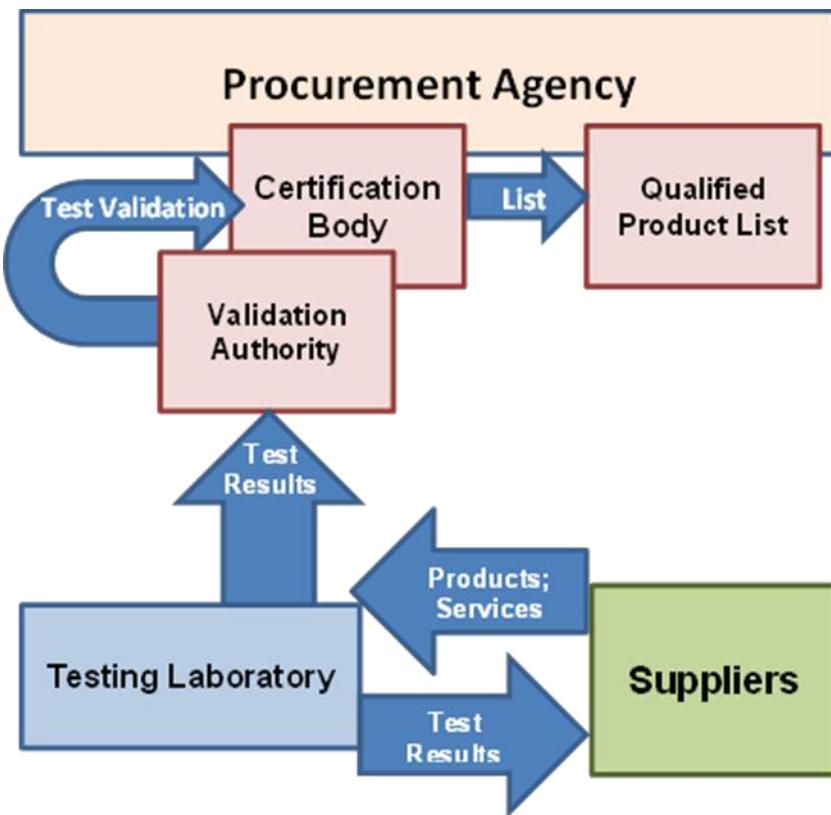


Figure 11 – Assessment Process

#### 6.2.4 CURRENT STATE OF CONFORMITY ASSESSMENT IN CLOUD COMPUTING

As described elsewhere in this document, standards specific to cloud computing are beginning to emerge, and several aspects of the conformance testing and conformity assessment processes described above are also starting to take place, conducted by a variety of organizations. In some cases, such as the CDMI, OCCI, OVF, and CIMI standards discussed below, industry-sponsored testing events and “plug-fests” are being advertised and conducted with participation from a variety of vendors and open source projects and community-based developers. In other cases, either the standards are not yet mature enough to permit such testing, or the participants have not yet exposed the conformity assessment processes to public view.

### 6.3 CATEGORIZING THE STATUS OF STANDARDS

Innovation in IT means that IT standards are constantly being developed, approved, and maintained. Revisions to previous editions of standards may or may not be backward-compatible. Table 4 – Standards Maturity Model provides an indication of the maturity level of a standard. Some SDOs require two or more implementations before final approval of a standard. Such implementations may or may not be commercially available products or services. In other cases, an SDO may be developing standards while commercial products or services are already being sold that conform to early drafts. (In such cases, companies take on the risk of creating products or services that may not conform to the final standard.)

Maturity Level	Definition
No Standard	SDOs have not initiated any standard development projects.
Under Development	SDOs have initiated standard development projects. Open source projects have been initiated.
Approved Standard	SDO-approved standard is available to public. Some SDOs require multiple implementations before final designation as a “standard.”
Technically Stable	The standard is stable and its technical content is mature. No major revisions or amendments are in progress that will affect backward compatibility with the original standard.
Reference Implementation	Reference implementation is available.
Testing	Test tools are available. Testing and test reports are available.
Commercial Availability	Several products/services from different vendors exist on the market to implement this standard.
Market Acceptance	Widespread use by many groups. De facto or de jure market acceptance of standards-based products/services.
Sunset	Newer standards (revisions or replacements) are under development.

Table 4 – Standards Maturity Model

## 6.4 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.

### 6.4.1 CLOUD STANDARDS FOR INTEROPERABILITY

Interoperability may be assessed in terms of the NIST Cloud Computing Reference Architecture 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 from Open Grid Forum and the Cloud Infrastructure Management Interface (CIMI) set from the Distributed Management Task Force (DMTF). 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 and also provides features that conform to DMTF’s Common Information Model (CIM). Each of these standard sets has seen significant uptake, and several available cloud system products either already implement or plan to implement at least one of them. While these IaaS standard sets are so far separate, OGF and DMTF have stated that they have a work register in place and that they continue to discuss the possibility of merging these efforts in the future.

In PaaS applications, an extensive ecosystem of vendor-specific products that are not interchangeable has emerged. A recent effort to produce a PaaS-specific standard<sup>22</sup> 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

---

<sup>22</sup> ID Cloud-PaaS <https://www.oasis-open.org/committees/download.../IDCloud-paas-v1c.odt>

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.

As appropriate, some of these interfaces will be tested and analyzed by NIST to validate their capabilities against the list of cloud computing use cases. Opportunities will also be made available for the vendor and open source community to demonstrate the applicability of standards and APIs to the defined NIST SAJACC cloud computing technical use cases.

#### 6.4.2 CLOUD COMPUTING 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 machine-readable 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.

#### 6.4.3 SUMMARY ON INTEROPERABILITY AND PORTABILITY

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”.

## 6.5 CLOUD COMPUTING STANDARDS FOR SECURITY

As noted in SP 800-146, “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.

## 6.6 CLOUD COMPUTING STANDARDS FOR PERFORMANCE

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
  - 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.

#### 6.6.1 CLOUD 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 WS-Agreement and WS-Agreement-Negotiation specifications from OGF. Recent work from an inter-SDO joint task force led by TM Forum has also produced a white paper<sup>23</sup> describing the

---

<sup>23</sup> <https://www.tmforum.org/WhitePapers/CloudMonetization/47730/article.html>

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.

#### 6.6.2 CLOUD STANDARDS FOR MONITORING

The situation with regard to cloud service monitoring is less well developed than for other areas due to the multiplicity of underlying products and the lack of a single set of well-defined monitoring and metric terms. To address this need, the NIST Cloud Computing Reference Architecture and Taxonomy group is developing a set of terms related to monitoring and metrics for service agreements, including SLAs.

The input from this group and from the TM Forum-led joint cross-SDO report discussed above will be used by the Business Use Case and SAJACC groups to develop use case scenarios that can be used to identify appropriate standards and standards gaps in this area.

ITU-T’s establishment of a cloud computing resource management area of study, a roadmap for the area of study and the initiation of related supporting standards, is beginning to address the closure of some of the standards gaps in cloud computing monitoring. The roadmap outlines the standards that are needed in order to monitor the health, QoS, and reliability of cloud services that are based on the aggregation of services from one or more cloud service providers.

#### 6.7 CLOUD COMPUTING STANDARDS FOR 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 [U.S. Access Board](#) is an independent federal agency devoted to accessibility for people with disabilities. The Access Board develops and maintains design criteria for the built environment, transit vehicles, telecommunications equipment, and for electronic and information technology. It

also provides technical assistance and training on these requirements and on accessible design and enforces accessibility standards that cover federally funded facilities.

Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), requires that Federal employees with disabilities have access to and use of information and data that are comparable to the access and use by federal employees who are not individuals with disabilities. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a federal agency, have access to and use of information and data that are comparable to that provided to the public who are not individuals with disabilities. Both of these requirements must be met unless an undue burden would be imposed on the agency.

Section 508 standards that would be applicable for many cloud computing applications are: Subpart B -- Technical Standards 1194.21 Software applications and operating systems; § 1194.22 Web-based intranet and internet information and applications; and 1194.23 Telecommunications products. The Access Board is in the process of revising the Section 508 standards. This is the first major revision since the standards were initially published in 2001. The initial product oriented approach to requirements is being replaced with a more functional approach. The Access Board plans to reference the W3C's Web Content Accessibility Guidelines (WCAG) 2.0 (<http://www.w3.org/TR/WCAG20/>), which is an international voluntary consensus guideline.

Additional voluntary consensus standards that may be applicable to cloud computing applications are: ISO 9241-20:2008, Ergonomics of human-system interaction -- Part 20: Accessibility guidelines for information/communication technology (ICT) equipment and services; ISO 9241-171:2008, Ergonomics of human-system interaction -- Part 171: Guidance on software accessibility; ANSI/HFES 200 Human Factors Engineering of Software User Interfaces (Parts 1, 2, and 3); and ISO/IEC 24751-1:2008, Information technology -- Individualized adaptability and accessibility in e-learning, education and training -- Part 1: Framework and reference model.

The White House released a memorandum *Strategy Plan for Improving Management of Section 508 of the Rehabilitation Act*, January 24, 2013<sup>24</sup>. The strategic plan provides a comprehensive and structured approach to further improve agencies' management of the requirements of Section 508. The objective is to ensure that all electronic and information technology (EIT) that is developed, procured, maintained, or used by the federal government is accessible, as required by Section 508 of the Rehabilitation Act of 1973.

---

<sup>24</sup> [www.whitehouse.gov/sites/default/files/omb/procurement/memo/strategic-plan-508-compliance.pdf](http://www.whitehouse.gov/sites/default/files/omb/procurement/memo/strategic-plan-508-compliance.pdf)

## 7 CLOUD COMPUTING STANDARDS MAPPING

One approach to cloud computing standards mapping is to map relevant standards using the conceptual model and the cloud computing taxonomy from the NIST Cloud Computing Reference Architecture and Taxonomy Working Group. As presented in Figure 12, the cloud computing conceptual model is depicted as an integrated diagram of system, organizational, and process components. The cloud computing taxonomy produced by the same working group has provided further categorizations for the security, interoperability, and portability aspects for cloud computing.

While many standards are generally relevant to these cloud computing areas, the following sections will map those specifically relevant cloud standards and capture their standard maturity status in a tabular format. The online cloud standards inventory (as described in Section 5) will be the place to maintain and track other relevant standards. Some standards may apply to more than one category from the cloud taxonomy and therefore may be listed more than once.

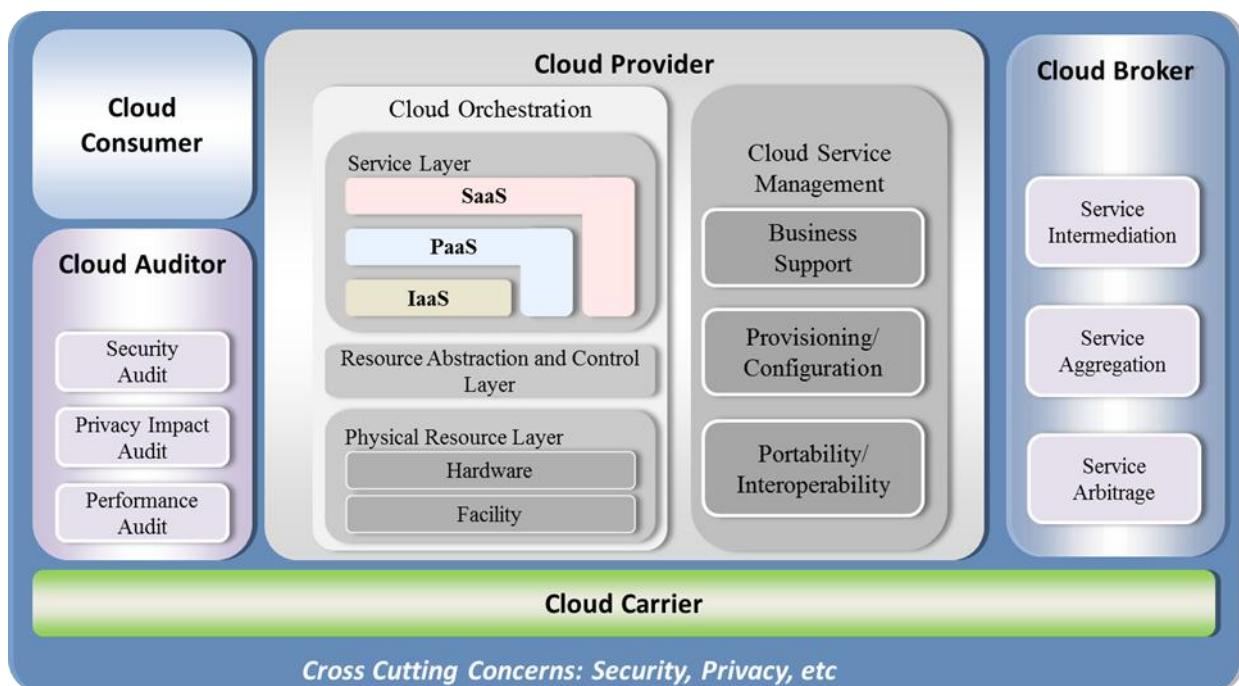


Figure 12 – The Combined Conceptual Reference Diagram

## 7.1 SECURITY STANDARDS MAPPING

The following tables map security standards to various security categories and list the status (ref: Section 6.3/ Table 4 – Standards Maturity Model). Some of the listed standards apply to more than one category and are therefore listed more than once.

Categorization	Available Standards	SDO	Status
<b>Authentication &amp; Authorization</b>	RFC 5246 Secure Sockets Layer (SSL)/ Transport Layer Security (TLS)	IETF	Approved Standard Market Acceptance
	RFC 3820: X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile	IETF	Approved Standard Market Acceptance
	RFC5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	IETF	Approved Standard Market Acceptance
	RFC 5849 OAuth (Open Authorization Protocol)	IETF	Approved Standard Market Acceptance
	ISO/IEC 9594-8:2008   X.509 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks	ISO/IEC & ITU-T	Approved Standard Market Acceptance
	ISO/IEC 29115   X.1254 Information technology -- Security techniques -- Entity authentication assurance framework	ISO/IEC & ITU-T	Approved Standard
	FIPS 181 Automated Password Generator	NIST	Approved Standard Market Acceptance
	FIPS 190 Guideline for the Use of Advanced Authentication Technology Alternatives	NIST	Approved Standard Market Acceptance
	FIPS 196 Entity Authentication Using Public Key Cryptography	NIST	Approved Standard Market Acceptance
	OpenID Authentication	OpenID	Approved Standard Market Acceptance
	eXtensible Access Control Markup Language (XACML)	OASIS	Approved Standard Market Acceptance
	Security Assertion Markup Language (SAML)	OASIS	Approved Standard Market Acceptance

**Table 5 – Security Standards: Authentication and Authorization**

Categorization	Available Standards	SDO	Status
<b>Confidentiality</b>	RFC 5246 Secure Sockets Layer (SSL)/ Transport Layer Security (TLS)	IETF	Approved Standard Market Acceptance
	Key Management Interoperability Protocol (KMIP)	OASIS	Approved Standard Market Acceptance
	XML Encryption Syntax and Processing	W3C	Approved Standard Market Acceptance
	FIPS 140-2 Security Requirements for Cryptographic Modules	NIST	Approved Standard Testing Market Acceptance
	FIPS 185 Escrowed Encryption Standard (EES)	NIST	Approved Standard Market Acceptance
	FIPS 197 Advanced Encryption Standard (AES)	NIST	Approved Standard Testing Market Acceptance
	FIPS 188 Standard Security Label for Information Transfer	NIST	Approved Standard Market Acceptance

Table 6 – Security Standards: Confidentiality

Categorization	Available Standards	SDO	Status
<b>Integrity</b>	XML signature (XMLDSig)	W3C	Approved Standard Market Acceptance
	FIPS 180-4 Secure Hash Standard (SHS)	NIST	Approved Standard Market Acceptance
	FIPS 186-4 Digital Signature Standard (DSS)	NIST	Approved Standard Market Acceptance
	FIPS 198-1 The Keyed-Hash Message Authentication Code (HMAC)	NIST	Approved Standard Market Acceptance

Table 7 – Security Standards: Integrity

Categorization	Available Standards	SDO	Status
<b>Identity Management</b>	X.idmcc Requirement of IdM in Cloud Computing	ITU-T	Under Development
	FIPS 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors	NIST	Approved Standard Market Acceptance
	Service Provisioning Markup Language (SPML)	OASIS	Approved Standard
	Web Services Federation Language (WS-Federation) Version 1.2	OASIS	Approved Standard
	WS-Trust 1.3	OASIS	Approved Standard
	Security Assertion Markup Language (SAML)	OASIS	Approved Standard Market Acceptance
	OpenID Authentication 1.1	OpenID Foundation	Approved Standard Market Acceptance

Table 8 – Security Standards: Identity Management

Categorization	Available Standards	SDO	Status
<b>Security Monitoring &amp; Incident Response</b>	ISO/IEC WD 27035-1  Information technology -- Security techniques -- Information security incident management -- Part 1: Principles of incident management	ISO/IEC	Under Development
	ISO/IEC WD 27035-3  Information technology -- Security techniques -- Information security incident management -- Part 3: Guidelines for CSIRT operations	ISO/IEC	Under Development
	ISO/IEC WD 27039; Information technology -- Security techniques -- Selection, deployment and operations of intrusion detection systems	ISO/IEC	Under Development
	ISO/IEC 18180  Information technology - Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2 (NIST IR 7275)	ISO/IEC	Approved Standard Market Acceptance
	X.1500  Cybersecurity information exchange techniques	ITU-T	Approved Standard Market Acceptance
	X.1520: Common vulnerabilities and exposures	ITU-T	Approved Standard
	X.1521  Common Vulnerability Scoring System	ITU-T	Approved Standard
	PCI Data Security Standard	PCI	Approved Standard Market Acceptance
	FIPS 191  Guideline for the Analysis of Local Area Network Security	NIST	Approved Standard Market Acceptance

Table 9 – Security Standards: Security Monitoring &amp; Incident Response

Categorization	Available Standards	SDO	Status
Security Controls	Cloud Controls Matrix Version 1.3	CSA	Approved Standard
	ISO/IEC 27001:2005  Information Technology – Security Techniques Information Security Management Systems Requirements	ISO/IEC	Approved Standard
	ISO/IEC WD TS 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	Under Development
	ISO/IEC 27018  Code of Practice for Data Protection Controls for Public Cloud Computing Services	ISO/IEC	Under Development
	ISO/IEC 1 <sup>st</sup> WD 27036-4  Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services	ISO/IEC	Under Development

Table 10 – Security Standards: Security Controls

Categorization	Available Standards	SDO	Status
<b>Security Policy Management</b>	ATIS-02000008 Trusted Information Exchange (TIE)	ATIS	Approved Standard Commercially Available
	FIPS 199 Standards for Security Categorization of Federal Information and Information Systems	NIST	Approved Standard Testing Market Acceptance
	FIPS 200 Minimum Security Requirements for Federal Information and Information Systems	NIST	Approved Standard Testing Market Acceptance
	ISO/IEC 27002 Code of practice for information security management	ISO/IEC	Approved Standard Market Acceptance
	eXtensible Access Control Markup Language (XACML)	OASIS	Approved Standard Market Acceptance

Table 11 – Security Standards: Security Policy Management

Categorization	Available Standards	SDO	Status
<b>Availability</b>	ATIS-02000009 Cloud Services Lifecycle Checklist	ATIS	Approved Standard
	ISO/PAS 22399:2007 Societal security - Guideline for incident preparedness and operational continuity management	ISO	Approved Standard Market Acceptance

Table 12 – Security Standards: Availability

## 7.2 INTEROPERABILITY STANDARDS MAPPING

As discussed in Section 6.3, 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 13 – Interoperability Standards.

Categorization	Available Standards	SDO	Status
Service Interoperability	Cloud Infrastructure Management Interface (CIMI)	DMTF	Approved Standard
	IEEE P2301, Draft Guide for Cloud Portability and Interoperability Profiles (CPIP)	IEEE	Under Development
	IEEE P2302, Draft Standard for Intercloud Interoperability and Federation (SIIF)	IEEE	Under Development
	Y.3520 Cloud computing framework for end to end resource management.	ITU-T	Approved Standard
	Cloud Application Management Platform (CAMP)	OASIS	Under Development
	Open Cloud Computing Interface (OCCI)	OGF	Approved Standard
	Data Format Description Language (DFDL)	OGF	Approved Standard
	Topology and Orchestration Specification for Cloud Applications (TOSCA), Version 1.0 Committee Specification Draft 06 / Public Review Draft 01	OASIS	Under Development
	Cloud Data Management Interface (CDMI) [Also approved as ISO/IEC 17826:2012, Information technology – Cloud Data Management Interface (CDMI)]	SNIA	Approved Standard Market Acceptance Commercially Available

Table 13 – Interoperability Standards

### 7.3 PORTABILITY STANDARDS MAPPING

As discussed in Section 6.4, 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.

Categorization	Available Standards	SDO	Status
<b>Data Portability</b>	Cloud Data Management Interface (CDMI)	SNIA	Approved Standard Market Acceptance Commercially Available
<b>System Portability</b>	Open Virtualization Format (OVF), OVF 1.0 [Also approved as INCITS 469-2010 & ISO/IEC 17203: 2011]	DMTF	Approved Standard Market Acceptance Commercial Availability
	Open Virtualization Format (OVF), OVF 2.0	DMTF	Approved Standard
	IEEE P2301 Draft Guide for Cloud Portability and Interoperability Profiles (CPIP)	IEEE	Under Development
	Topology and Orchestration Specification for Cloud Applications (TOSCA), Version 1.0 Committee Specification Draft 06 / Public Review Draft 01	OASIS	Under Development

Table 14 – Portability Standards

#### 7.4 PERFORMANCE STANDARDS MAPPING

As discussed in Section 6.6, performance standards are needed for cloud service agreements and for cloud service monitoring, Table 15 – Performance Standards provides a list of current standards that may be considered.

Categorization	Available Standards	SDO	Status
<b>Service Agreements</b>	Topology and Orchestration Specification for Cloud Applications (TOSCA), Version 1.0 Committee Specification Draft 06 / Public Review Draft 01	OASIS	Under Development
	GB917 SLA Management Handbook, Release 3.1	TM Forum	Approved Standard
	GB963 Cloud SLA Application Note, Version 1.2	TM Forum	Approved Standard
	TR178 Enabling End-to-End Cloud SLA Management, Version 0.4	TM Forum	Approved Standard
	TR194 Multi-Cloud Service Management Accelerator Pack - Introduction, Release 1.0	TM Forum	Approved Standard
	TR195 Multi-Cloud Service Management Pack - Business Guide, Release 1.0	TM Forum	Approved Standard
	TR196 Multi-Cloud Service Management Pack - Technical Guide, Release 1.0	TM Forum	Approved Standard
	TR197 Multi-Cloud Service Management Pack – SLA Business Blueprint	TM Forum	Approved Standard
	TR198 Multi-Cloud Service Management Pack – Developer Primer	TM Forum	Approved Standard

Table 15 – Performance Standards

## 7.5 ACCESSIBILITY STANDARDS MAPPING

As discussed in Section 6.7, adherence to Section 508 accessibility standards would be required for many federal cloud computing applications. The Section 508 standards are being revised and are incorporating international voluntary consensus standards. The following table lists accessibility standards, which may be relevant for federal cloud computing applications.

Categorization	Available Standards	SDO	Status
<b>Accessibility</b>	Section 508 standards (Technical Standards 1194.21 Software applications and operating systems; § 1194.22 Web-based intranet and internet information and applications; and 1194.23 Telecommunications products)	US Access Board	Approved Standard Market Acceptance Under Revision
	W3C Web Content Accessibility Guidelines (WCAG) 2.0	W3C	Approved Standard Market Acceptance
	ISO 9241-20:2008, Ergonomics of human-system interaction -- Part 20: Accessibility guidelines for information/communication technology (ICT) equipment and services	ISO/IEC	Approved Standard
	ISO 9241-171:2008, Ergonomics of human-system interaction -- Part 171: Guidance on software accessibility	ISO/IEC	Approved Standard
	ISO/IEC 24751-1:2008, Information technology -- Individualized adaptability and accessibility in e-learning, education and training -- Part 1: Framework and reference model	ISO/IEC	Approved Standard
	ANSI/HFES 200 Human Factors Engineering of Software User Interfaces (Parts 1, 2, and 3)	ANSI	Approved Standard

Table 16 – Accessibility Standards

## 8 ANALYZING USE CASES TO IDENTIFY STANDARDS GAPS

There are several facets of cloud service interfaces that are candidates for standardization including:

- Management APIs;
- Data Exchange Formats;
- Federated Identity and Security Policy APIs;
- Resource Descriptions; and
- Data Storage APIs.

With these candidate areas in mind, the following business use cases can be analyzed with regard to their possible deployment modes (as discussed in Section 4.3) to identify required standards. This analysis, in conjunction with the NIST Cloud Standards Inventory, enables the availability of relevant existing and emerging standards to be evaluated. Where no suitable standards of any kind exist, this is a gap. The priority of the standards or requirements in question is also identified.

### 8.1 USE CASE: CREATING, ACCESSING, UPDATING, DELETING DATA OBJECTS IN CLOUD SYSTEMS

Benefits: Cross-cloud system applications

Deployment Mode Considerations: Basic Create-Read-Update-Delete (CRUD) operations on data objects will primarily be done between a single client and provider, and should observe any required standards for authentication and authorization.

Standardization Needed: Standard interfaces to metadata and data objects

Possible Standards: CDMI from SNIA

**8.2 USE CASE: MOVING VMS, VIRTUAL APPLIANCES, SERVICES, AND APPLIANCES BETWEEN CLOUDS**

Benefits: Migration, Hybrid Clouds, Disaster Recovery, Cloudbursting

Deployment Mode Considerations: When moving a VM out of one cloud system and into another as two separate actions, conceivably two different ID management systems could be used. When moving VMs in a truly hybrid cloud, however, federated ID management standards will be needed.

Standardization Needed: Common VM description format, common service and application description format

Possible Standards: OVF from DMTF, TOSCA from OASIS, OpenID, OAuth

**8.3 USE CASE: SELECTING THE BEST IAAS CLOUD VENDOR, PUBLIC OR PRIVATE**

Benefits: Provide cost-effective reliable deployments

Deployment Mode Considerations: When considering hybrid or distributed (inter)cloud deployments, uniform and consistent resource, performance, and policy descriptions are needed.

Standardization Needed: Resource and performance requirements description languages.

Possible Standards: For basic resource descriptions, DMTF CIM and OGF GLUE are candidates. Other, more extensive description languages for performance or policy enforcement are to be determined. For Master Service Agreements and Service Level Agreements, WS-Agreement and WS-Agreement-Negotiation (WS-AG, WS-AN) from OGF; for cloud application and service level description of attributes, relationships, requirements, and capabilities, TOSCA from OASIS.

**8.4 USE CASE: PORTABLE TOOLS FOR MONITORING AND MANAGING CLOUD SYSTEMS**

Benefits: Simplifies operations as opposed to individual tools for each cloud

Deployment Mode Considerations: Monitoring and managing are separate but closely related tasks. The standards required will differ depending on whether the monitoring and managing must be done across trust boundaries or across distributed environments.

Standardization Needed: Standard monitoring and management interfaces to IaaS resources

Possible Standards: Cloud IaaS management standards include CIMI from DMTF and OCCI from OGF; OCCI has also been successfully applied to management of aggregated federated cloud systems. PaaS APIs vary widely, but CAMP from OASIS has begun standardization work in this area. SaaS standardization on data formats and exchange protocols may be possible. Basic monitoring standards exist, such as the Syslog Protocol (IETF RFC 5424), which can be used with the Transport Layer Security (TLS) Transport Mapping for Syslog (IETF RFC 5425). Basic management standards include the Cloud Management WG from DMTF, and OCCI from OGF.

- An Overview of the IETF Network Management Standards (IETF RFC 6632)
- Simple Network Management Protocol or SNMP (IETF RFC 3411)
- IP Flow Information eXport or IPFIX (IETF RFC 5101)
- Network Configuration Protocol or NETCONF (IETF RFC 6241)
- WS-AG and WS-AN for expression of service agreement monitoring parameters and units and for expression of remedy terms and negotiation parameters.

#### 8.5 USE CASE: MOVING DATA BETWEEN CLOUD SYSTEMS

Benefits: Migration between cloud systems, cross-cloud application, and B2B integration

Deployment Mode Considerations: Migrating data from one cloud system to another in two separate moves through the client is a simpler case. Migrating data directly from one cloud system to another will require standards for federated identity, delegation of trust, and secure third-party data transfers.

Standardization Needed: Standard metadata/data formats for movement between cloud systems

Standardized query languages (e.g., for NoSQL for IaaS)

Possible Standards: AS4, OAGIS, NoSQL, GridFTP, DFDL, CDMI

**8.6 USE CASE: SINGLE SIGN-ON ACCESS TO MULTIPLE CLOUD SYSTEMS**

Benefits: Simplified access, cross-cloud applications

Deployment Mode Considerations: Single sign-on can mean using the same credentials to access different cloud systems independently at different times. Single sign-on to access an inter-cloud application that spans multiple cloud systems will require federated identity management, delegation of trust, and virtual organizations.

Standardization Needed: Federated identity, authorization, and virtual organizations

Possible Standards: OpenID, OAuth, SAML, WS-Federation and WS-Trust, CSA outputs; Virtual Organization Management System (VOMS) from OGF.

**8.7 USE CASE: ORCHESTRATED PROCESSES ACROSS CLOUD SYSTEMS AND ENTERPRISE SYSTEMS**

Benefits: Direct support for necessarily distributed systems

Deployment Mode Considerations: This use case is inherently distributed and across trust boundaries. This can be generally termed federated resource management and is a central concept in the grid computing community. The term inter-cloud can also be used to denote this concept.

Standardizations Needed: To address this use case completely, an entire set of capabilities need to be standardized, e.g.:

- Infrastructure services;
- Execution Management services;
- Data services;
- Resource Management services;
- Security services;
- Self-management services; and
- Information services.

Possible Standards: SOA standards (such as WS-I) and grid standards (such as the OGSA WSRF Basic Profile, OGF GFD-R-P.072) exist that cover these areas, but issues around stateful resources, callbacks/notifications, and remote content lifetime management has caused these to be eclipsed by the simplicity of Representational State Transfer (REST). Hence, standard, REST-based versions of these capabilities must be developed. Such work is being done in several organizations, including the IEEE.

DMTF and OGF. The OGF Distributed Computing Infrastructure Federations Working Group (DCI Federal [DCIfed]-WG) is addressing two usage scenarios: (1) delegation of workload from one domain into the other, covering job description, submission, and monitoring; and (2) leasing of resources, including resource definition, provisioning, and monitoring. Existing standards to support this include WS-Agreement, Job Submission Description Language, GLUE, OGSA Basic Execution Service, OCCI, and Usage Record. Specific business application data formats may be supported by OASIS.

Workflow and workflow engines will also need standardization and adoption in the cloud arena. BPEL is one existing standard but extensions might be needed to efficiently support scientific and engineering workflows.

## 8.8 USE CASE: DISCOVERING CLOUD RESOURCES

Benefits: Selection of appropriate cloud systems for applications

Deployment Mode Considerations: To support inter-cloud resource discovery, secure federated catalog standards are needed.

Standardization Needed: Description languages for available resources, Catalogue interfaces

Possible Standards: This use case addresses two areas of standardization: (1) description languages for the resources to be discovered, and (2) the discovery APIs for the discovery process itself. Some existing standards and tools cover both areas. RDF is a standard formalism for describing resources as triples consisting of subject-predicate-object. The Dublin Core is a small fundamental set of text elements for describing resources of all types. It is commonly expressed in RDF. Since the Dublin Core is a “core” set, it is intended to be extensible for a broad range of application domains.

Such work is being pursued by the Dublin Core Metadata Initiative. ebXML Registry Information Model (ebRIM) actually defines both a description language and a discovery method, ebXML Registry Services (ebRS).

ID-WSF also defines both a discovery information model and discovery services that cover federated identity and access management. LDAP is an existing standard that has been used to build catalogue and discovery services, but issues might occur with regards to read vs. write optimization. UDDI is another existing standard from OASIS. A third existing standard is CSW from OGC that

uses ebRIM. While this was originally developed to support geospatial applications, it is widely used in distributed catalogues that include services. All of these existing standards need to be evaluated for suitability for cataloguing and discovery of cloud resources and services.

#### 8.9 USE CASE: EVALUATING SLAS AND PENALTIES

Benefits: Selection of appropriate cloud resources

Deployment Mode Considerations: SLAs will be primarily established between a single client and provider, and should observe any required standards for authentication, authorization, and non-repudiation. The need for SLAs between a single client but across multiple providers will be much less common. The difficulty in effectively implementing distributed SLAs will also discourage their development.

Standardization Needed: SLA description language

Possible Standards: WS-Agreement (GFD.107) defines a language and a protocol for advertising the capabilities of service providers and creating agreements based on creational offers, and for monitoring agreement compliance at runtime. This is supported by WS-AgreementNegotiation (OGF), which defines a protocol for automated negotiation of offers, counter offers, and terms of agreements defined under WS-Agreement-based service agreements.

#### 8.10 USE CASE: AUDITING CLOUD SYSTEMS

Benefits: Ensure regulatory compliance. Verify information assurance.

Deployment Mode Considerations: Auditing will be done primarily between a single client and provider, and should observe any required standards for authentication, authorization, integrity, and non-repudiation.

Standardization Needed: Auditing standards and verification check lists

Possible Standards: CSA Cloud Audit. Relevant informational work can be found in Guidelines for Auditing Grid Certificate Authorities (OGF GFD.169).

**8.11 END-TO-END: CLOUD RESOURCE MANAGEMENT USE CASE**

Benefits: Supports customer service in a multi-cloud service provider environment.

Deployment/Management Mode Considerations: This use case involves the management of end-to-end health and QoS of the services offered by a cloud service provider that involves the integration of several base services offered by multiple cloud service providers, forming composite cloud services and applications.

Standardizations Needed: A framework for multi-cloud resource and service management that support the manageability for a single cloud service as well as for multiple cloud services

Possible Standards: In order for the composite cloud computing services to work effectively, all the prerequisite services within the multi-cloud service system must function properly, and when a problem occurs, the service must be restored rapidly and easily. In this use case, there are the two types of connection paths, namely Service Delivery Path and Service Management Path. When the cloud consumer is experiencing a problem with an application service and contacts a cloud service provider support center, the cloud service provider should have visibility into the health and welfare of the cloud service provider application service, its underlying cloud infrastructure, as well as the local service provider's network management systems relevant to the voice application service (i.e., end-to-end cloud resource management). Standards are needed that would offer ways to build such end-to-end and manageable multi-cloud solutions.

## 9 USG PRIORITIES TO FILL 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.

### 9.1 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.

#### 9.1.1 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.

#### 9.1.2 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.

#### 9.1.3 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 cloud-based hosting system. However, data format for backup and migration of application workload, including database serialization/de-serialization, need further standardization to support portability.

#### 9.1.4 BUSINESS SUPPORT, PROVISIONING AND CONFIGURATION

In cloud service management areas, the importance of standard data formats and interfaces to describe service-level agreement (SLA) and quality of service (QoS) in traditional IT systems is high. While standards do exist for SLA negotiation and automated service condition matching, the application of these to the fine level of detail expected for large-scale cloud use cases is just developing. Computing resource description and discovery are also in need of standardization as consumers transition from buying and managing resources to renting resources in a cloud system.

This is limited not only to raw computing resources such as virtualized processing, storage, and networking resources, but also includes higher-level abstractions of application processing resources. A standardization gap identified in a related area is metering and billing of service consumptions; data formats and management interfaces are used to report, deliver, and communicate this usage information.

#### 9.1.5 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.

#### 9.1.6 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.)

## 9.2 STANDARDIZATION PRIORITIES BASED ON USG 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 for USG cloud consumers:

### 9.2.1 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.

#### 9.2.2 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.

#### 9.2.3 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 groups<sup>25</sup> 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.

#### 9.2.4 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.

---

<sup>25</sup> <https://www.fbo.gov/utils/view?id=4c4e37f4f1bcd2cb8d0a16f0e1b0ddbe>

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

#### 9.2.5 SUMMARY OF STANDARDIZATION GAPS AND STANDARDIZATION PRIORITIES

Table 17 – Areas of Standardization Gaps and Standardization Priorities provides a mapping of present standards gaps and how they relate to USG high priorities.

Area of Standardization Gaps	High Priorities for Standardization Based On USG Requirements
SaaS Functional Interfaces (9.1.1 / page 70), e.g., <ul style="list-style-type: none"> <li>- Data format and interface standards for email and office productivity</li> <li>- Metadata format and interface standards for e-discovery</li> </ul>	High standardization priorities on: <ul style="list-style-type: none"> <li>- SaaS application specific data and metadata format standards to support interoperability and portability requirement when migrating high-value, low-risk applications to SaaS (Section 9.2.3).</li> </ul>
SaaS Self-Service Management Interfaces (Section 9.1.2), e.g., <ul style="list-style-type: none"> <li>- Interface standards related to user account and credential management</li> </ul>	Not a high standardization priority at this time
PaaS Functional Interfaces (Section 9.1.3), e.g., <ul style="list-style-type: none"> <li>- Standards of data format to support database serialization and de-serialization</li> </ul>	Not a high standardization priority at this time
Business Support, Provisioning and Configuration (Section 9.1.4), e.g., <ul style="list-style-type: none"> <li>- Standards for describing cloud service-level agreement and quality of services</li> <li>- Standards for describing and discovering cloud service resources</li> <li>- Standards for metering and billing of service consumptions and usage</li> </ul>	High standardization priorities on: <ul style="list-style-type: none"> <li>- Resource description and discovery standards to support data center consolidation using private and community IaaS cloud systems (Section 9.2.4)</li> </ul>

Area of Standardization Gaps	High Priorities for Standardization Based On USG Requirements
<p>Security (Section 9.1.5), e.g.,</p> <ul style="list-style-type: none"> <li>- Standards for identity provisioning and management across different network and administration domains</li> <li>- Standards for secure and efficient replication of identity and access policy information across systems</li> <li>- Single Sign-On interface and protocol standards that support strong authentication</li> <li>- Standards in policies, processes, and technical controls in supporting the security auditing, regulation, and law compliance needs</li> </ul>	<p>High standardization priorities on:</p> <ul style="list-style-type: none"> <li>- Security auditing and compliance standards to support secure deployment, assess, and accreditation process for cloud-specific deployment (Section 9.2.1)</li> <li>- Identity and access management standards to support secure integration of cloud systems into existing enterprise security infrastructure (Section 9.2.2)</li> </ul>
<p>Accessibility (Section 9.1.6), e.g.</p> <ul style="list-style-type: none"> <li>- Standardized “framework” for exchanging an individual’s accessibility requirements</li> </ul>	<p>Not a high standardization priority at this time</p>

**Table 17 – Areas of Standardization Gaps and Standardization Priorities**

## 10 CONCLUSIONS AND RECOMMENDATIONS

### 10.1 CONCLUSIONS

Cloud computing can enable USG agencies to achieve cost savings and increased ability to quickly create and deploy enterprise applications. While cloud computing technology challenges many traditional approaches to data center and enterprise application design and management, requirements for accessibility, interoperability, performance, portability, and security remain critically important for successful deployments. Technically sound and timely standards are instrumental to ensuring that requirements for interoperability, portability, and security are met.

There is a fast-changing landscape of cloud computing-relevant standardization under way in a number of SDOs. While there are only a few approved cloud computing-specific standards at present, USG agencies should be encouraged to participate in specific cloud computing standards development projects that support their priorities in cloud computing services.

### 10.2 RECOMMENDATION TO USG AGENCIES TO HELP ACCELERATE THE DEVELOPMENT AND USE OF CLOUD COMPUTING STANDARDS

USG laws and policies encourage federal agency participation in the development and use of voluntary consensus standards and in conformity assessment activities. The following recommendations provide further guidance on how agencies can help to accelerate the development and use of cloud computing standards.

#### **Recommendation 1 – Contribute Agency Requirements**

Agencies should coordinate and contribute clear and comprehensive user requirements for cloud computing standards projects.

#### **Recommendation 2 – Participate in Standards Development**

Agencies should actively participate and coordinate in cloud computing standards development projects that are of high priority to their agency missions. The January 17, 2012, White House Memorandum, M-12-08, lists five fundamental strategic objectives for federal government agencies whenever engaging in standards development:

- Produce timely, effective standards and efficient conformity assessment schemes that are essential to addressing an identified need;
- Achieve cost-efficient, timely, and effective solutions to legitimate regulatory, procurement, and policy objectives;

- Promote standards and standardization systems that promote and sustain innovation and foster competition;
- Enhance U.S. growth and competitiveness and ensure non-discrimination, consistent with international obligations; and
- Facilitate international trade and avoid the creation of unnecessary obstacles to trade.

**Recommendation 3 – Encourage Testing to Accelerate Technically Sound Standards-Based Deployments**

Agencies should support the concurrent development of conformity and interoperability assessment schemes to accelerate the development and use of technically sound cloud computing standards and standards-based products, processes, and services. Agencies should also include consideration of conformity assessment approaches currently in place that take account of elements from international systems, to minimize duplicative testing and encourage private sector support.

**Recommendation 4 – Specify Cloud Computing Standards**

Agencies should specify cloud computing standards in their procurements and grant guidance when multiple vendors offer standards-based implementations and there is evidence of successful interoperability testing.

**Recommendation 5 – USG-Wide Use of Cloud Computing Standards**

To support USG requirements for accessibility, interoperability, performance, portability, and security in cloud computing, the Federal Cloud Computing Standards and Technology Working Group, in coordination with the Federal CIO Council Cloud Computing Executive Steering Committee (CCESC) and the Cloud First Task Force, should recommend specific cloud computing standards and best practices for USG-wide use.

## 11 BIBLIOGRAPHY

This section provides sources for additional information.

### Distributed Management Task Force (DMTF)

- Interoperable Clouds White Paper  
DSP-IS0101 Cloud Interoperability White Paper V1.0.0

This white paper describes a snapshot of the work being done in the DMTF Open Cloud Standards Incubator, including use cases and reference architecture as they relate to the interfaces between a cloud service provider and a cloud service consumer.  
[http://dmtf.org/sites/default/files/standards/documents/DSP-IS0101\\_1.0.0.pdf](http://dmtf.org/sites/default/files/standards/documents/DSP-IS0101_1.0.0.pdf)

- Architecture for Managing Clouds White Paper  
DSP-IS0102 Architecture for Managing Clouds White Paper V1.0.0

This white paper is one of two Phase 2 deliverables from the DMTF Cloud Incubator and describes the reference architecture as it relates to the interfaces between a cloud service provider and a cloud service consumer. The goal of the Incubator is to define a set of architectural semantics that unify the interoperable management of enterprise and cloud computing.  
[http://dmtf.org/sites/default/files/standards/documents/DSP-IS0102\\_1.0.0.pdf](http://dmtf.org/sites/default/files/standards/documents/DSP-IS0102_1.0.0.pdf)

- Use Cases and Interactions for Managing Clouds White Paper  
DSP-IS0103 Use Cases and Interactions for Managing Clouds White Paper V1.0.0

This document is one of two documents that together describe how standardized interfaces and data formats can be used to manage clouds. The document focuses on use cases, interactions, and data formats. [http://dmtf.org/sites/default/files/standards/documents/DSP-IS0103\\_1.0.0.pdf](http://dmtf.org/sites/default/files/standards/documents/DSP-IS0103_1.0.0.pdf)

### Global Inter-Cloud Technology Forum (GICTF)

Use Cases and Functional Requirements for Inter-Cloud Computing  
Published on August 2010  
[http://www.gictf.jp/doc/GICTF\\_Whitepaper\\_20100809.pdf](http://www.gictf.jp/doc/GICTF_Whitepaper_20100809.pdf)

This white paper describes three areas of advantages of inter-cloud computing, which are assured or prioritized performance, availability, and convenience of combined services. Several use cases of inter-cloud computing are provided with details according to these three areas, such as assured performance against transient overload, disaster recovery and service continuity for availability, and federated service provisions, followed by sequential procedures and functional requirements for each use case. Essential functional entities and interfaces are identified to meet these described requirements.

Technical Requirements for Supporting the Intercloud Networking

Published on April 2012

[http://www.gictf.jp/doc/GICTF\\_NWSWG-WhitePaper\\_e\\_20120420.pdf](http://www.gictf.jp/doc/GICTF_NWSWG-WhitePaper_e_20120420.pdf)

Based on the preceding Inter-Cloud use cases and functional requirements, this white paper describes technical requirements for each use case such as assured service level, disaster recovery, service continuity, and federated service provisions.

It also shows expected technical evolutions in a next few years.

### **TM Forum**

Cloud Monetization Differentiating Cloud Services

Released: January 2012

<https://www.tmforum.org/WhitePapers/CloudMonetization/47730/article.html>

This whitepaper explores the various cloud bill requirements and complexities for the different cloud business models. It will also explore the expectations from customers of cloud services, with respect to billing for cloud services, highlighting gaps and potential risks to service provider success, as well as recommend areas for further action.

**12 APPENDIX A – NIST FEDERAL INFORMATION PROCESSING STANDARDS AND SPECIAL PUBLICATIONS RELEVANT TO CLOUD COMPUTING**

[Federal Information Process Standards Publication \(FIPS\) 199, Standards for Security Categorization of Federal Information and Information Systems](#)

[Federal Information Processing Standards Publication \(FIPS\) 200, Minimum Security Requirements for Federal Information and Information Systems](#)

[NIST Special Publication 500-292, NIST Cloud Computing Reference Architecture, September 2011](#)

[NIST Special Publication 500-293, U.S. Government Cloud Computing Technology Roadmap, Release 1.0 \(Draft\), Volume I High-Priority Requirements to Further USG Agency Cloud Computing Adoption, November 2011](#)

[NIST Special Publication 500-293, U.S. Government Cloud Computing Technology Roadmap, Release 1.0 \(Draft\), Volume II Useful Information for Cloud Adopters, November 2011](#)

[NIST Special Publication 800-37 Rev.1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach](#)

[NIST Special Publication 800-53 Rev.4, Security and Privacy Controls for Federal Information Systems and Organizations](#)

[NIST Special Publication 800-53 Rev.3, Recommended Security Controls for Federal Information Systems and Organizations](#)

[NIST Special Publication 800-92, Guide to Computer Security Log Management](#)

[NIST Special Publication 800-125, Guide to Security for Full Virtualization Technologies](#)

[NIST Special Publication 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations](#)

[NIST Special Publication 800-144, Guidelines on Security and Privacy Issues in Public Cloud Computing](#)

[NIST Special Publication 800-145, The NIST Definition of Cloud Computing](#)

[NIST Special Publication 800-146, Cloud Computing Synopsis and Recommendations](#)

## 13 APPENDIX B – DEFINITIONS

**Accreditation** - Third-party attestation related to a conformity assessment body conveying formal demonstration of its competence to carry out specific conformity assessment tasks [SOURCE: ISO/IEC 17000:2004, Conformity assessment — Vocabulary and general principles]

### Accessibility

– Measurable characteristics that indicate the degree to which a system is available to, and usable by, individuals with disabilities. The most common disabilities include those associated with vision, hearing, and mobility, as well as cognitive disabilities.

[SOURCE: This report]

– Usability of a product, service, environment or facility by individuals with the widest range of capabilities

NOTE 1 issues.

Although "accessibility" typically addresses users who have a disability, the concept is not limited to disability.

NOTE 2 Adapted from ISO/TS 16071:2003, Ergonomics of human-system interaction -- Guidance on accessibility for human-computer interfaces

[SOURCE: ISO/IEC 24751-1:2008, Information technology -- Individualized adaptability and accessibility in e-learning, education and training -- Part 1: Framework and reference model]

**Attestation** – Issue of a statement, based on a decision following review that fulfillment of specified requirements has been demonstrated

[SOURCE: ISO/IEC 17000:2004, Conformity assessment — Vocabulary and general principles]

**Certification** – Third-party attestation related to products, processes, systems or persons.

NOTE 1 Certification of a management system is sometimes also called registration.

NOTE 2 Certification is applicable to all objects of conformity assessment except for conformity assessment bodies themselves, to which accreditation is applicable.

[SOURCE: ISO/IEC 17000:2004, Conformity assessment — Vocabulary and general principles]

**Conformity assessment** – Demonstration that specified requirements relating to a product process, system, person or body are fulfilled [ISO/IEC 17000:2004, Conformity assessment — Vocabulary and general principles]

[SOURCE: Guidance on Federal Conformity Assessment Activities

<http://gsi.nist.gov/global/index.cfm/L1-5/L2-45/A-332>

[SOURCE: The ABC's of the U.S. Conformity Assessment System

<http://gsi.nist.gov/global/index.cfm/L1-5/L2-45/A-337>

**First-party conformity assessment activity** – Conformity assessment activity that is performed by the person or organization that provides the object

NOTE: The first-, second- and third-party descriptors used to characterize conformity assessment activities with respect to a given object are not to be confused with the legal identification of the relevant parties to a contract.

[SOURCE: ISO/IEC 17000:2004, Conformity assessment — Vocabulary and general principles]

**Data Migration** – The periodic transfer of data from one hardware or software configuration to another or from one generation of computer technology to a subsequent generation. Migration is a necessary action for retaining the integrity of the data and for allowing users to search, retrieve, and make use of data in the face of constantly changing technology.

[SOURCE : <http://www.ischool.utexas.edu/~scisco/lis389c.5/email/gloss.html>]

**Information Technologies (IT)** – Encompasses all technologies for the capture, storage, retrieval, processing, display, representation, organization, management, security, transfer, and interchange of data and information.

[SOURCE: This report]

**Interoperability** – The capabilities to communicate, execute programs, or transfer data among various functional units under specified conditions.

[SOURCE: [American National Standard Dictionary of Information Technology \(ANSGIT\)](#)]

**Maintainability** – A measure of the ease with which maintenance of a functional unit can be performed using prescribed procedures and resources. Synonymous with serviceability. [SOURCE: [American National Standard Dictionary of Information Technology \(ANSGIT\)](#)]

**Network Resilience** – A computing infrastructure that provides continuous business operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged), rapid recovery if failure does occur, and the ability to scale to meet rapid or unpredictable demands.

[SOURCE: The Committee on National Security Systems Instruction No 4009,"National Information Assurance Glossary." CNSSI-4009]

**Performance** – The ability to track service and resource usage levels and to provide feedback on the responsiveness and reliability of the network.

[SOURCE: ETSI and 3GPP Dictionary]

**Portability** – The capability of a program to be executed on various types of data processing systems with little or no modification and without converting the program to a different language.

[SOURCE: [American National Standard Dictionary of Information Technology \(ANSGIT\)](#)]

- 1) The ability to transfer data from one system to another without being required to recreate or reenter data descriptions or to modify significantly the application being transported.
- 2) The ability of software or of a system to run on more than one type or size of computer under more than one operating system.

[SOURCE: [Federal Standard 1037C, Glossary of Telecommunication Terms](#), 1996]

**Privacy** – Information privacy is the assured, proper, and consistent collection, processing, communication, use, and disposition of personal information (PI) and personally identifiable information (PII) throughout its life cycle.

[SOURCE: NIST Cloud Computing Reference Architecture and Taxonomy Working Group]

**Reference implementation** – An implementation of a standard to be used as a definitive interpretation for the requirements in that standard. Reference implementations can serve many purposes. They can be used to verify that the standard is implementable, validate conformance test tools, and support interoperability testing among other implementations. A reference implementation may or may not have the quality of a commercial product or service that implements the standard.

[SOURCE: This report]

**Reliability** – A measure of the ability of a functional unit to perform a required function under given conditions for a given time interval.

[SOURCE: [American National Standard Dictionary of Information Technology \(ANSGIT\)](#)]

A time server / time service provides accurate and **reliable** network time where various vendor's products are calibrated to NIST's Time Server / Time Service, for example in wide area computing **TIME** sharing, metrics and metering of computational node, cloud center traversals using industry standard groups protocols such as IEEE C37.118, IEC 61850, and IEEE 802.1AG for execution management, governance of execution run time where a reference time stamp marks the scheduling, e.g., start, stop and time to live of a run time service or distributed algorithm.

## Resilience

- The ability to reduce the magnitude and/or duration of disruptive events to critical infrastructure. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event. [SOURCE: [Critical Infrastructure Resilience Final Report and Recommendations, National Infrastructure Advisory Council, September 8, 2009](#)]

- The adaptive capability of an organization in a complex and changing environment.

[SOURCE: ASIS International, ASIS SPC.1-2009, American National Standard, Organizational Resilience: Security, Preparedness, and Continuity Management System – Requirements with Guidance for Use.]

**Risk Management** – Coordinated activities to direct and control an organization with regard to risk ISO/IEC 27005, Information Technology – Security Techniques – Information Security Risk Management

**Second-party conformity assessment activity** – Conformity assessment activity that is performed by a person or organization that has a user interest in the object

[ISO/IEC 17000:2004, Conformity assessment — Vocabulary and general principles]

**Security** – Refers to information security. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

- Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;
- Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- Availability, which means ensuring timely and reliable access to and use of information.

[SOURCE: [Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002 \(FISMA\)](#)]

## Standard

– A document, established by consensus and approved by a recognized body that provides for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context. Note: Standards should be based on the consolidated results of science, technology, and experience, and aimed at the promotion of optimum community benefits.

[SOURCE: ISO/IEC Guide 2:2004, Standardization and related activities – General Vocabulary, definition 3.2]

– A document that may provide the requirements for: a product, process or service; a management or engineering process; or a testing methodology. An example of a product standard is the multipart ISO/IEC 24727, *Integrated circuit card programming interfaces*. An example of a management process standard is the ISO/IEC 27000, *Information security management systems*, family of standards. An example of an engineering process standard is ISO/IEC 15288, System life cycle processes. An example of a testing methodology standard is the multipart ISO/IEC 19795, *Biometric Performance Testing and Reporting*.

**Standards Developing Organization (SDO)** – Any organization that develops and approves standards using various methods to establish consensus among its participants. Such organizations may be: accredited, such as ANSI-accredited IEEE; or international treaty-based, such as the ITU-T; or international private sector-based, such as ISO/IEC; or an international consortium, such as OASIS or IETF; or a government agency.

SOURCE: [This report]

**Third-party conformity assessment activity** – Conformity assessment activity that is performed by a person or body that is independent of the person or organization that provides the object and user interests in that object

[SOURCE: ISO/IEC 17000:2004, Conformity assessment — Vocabulary and general principles]

**Test** – Technical operation that consists of the determination of one or more characteristics of a given product, process or service according to a specified procedure. [ISO/IEC Guide 2:2004]

**Testing** – Action of carrying out one or more tests. [ISO/IEC Guide 2:2004]

**Usability** – The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use.

[SOURCE: ISO 9241-11:1998 Ergonomic requirements for office work with visual display terminals (VDTs) – Part 11: Guidance on usability and ISO/IEC 25062:2006 Software engineering – Software product Quality Requirements and Evaluation (SquaRE) – Common Industry Format (CIF) for usability test reports]

**14 APPENDIX C – ACRONYMS**

**ANSGIT** American National Standard Dictionary of Information Technology

**API** Application Programming Interface

**BOD** Business Object Document

**CCESC** Cloud Computing Executive Steering Committee

**CDMI** Cloud Data Management Interface

**CDN** Content Delivery Network

**CIMI** Cloud Infrastructure Management Interface

**CIO** Chief Information Officer

**CMWG** Cloud Management Working Group

**COTS** Commercial off-the-shelf

**CPU** Central Processing Unit

**CRM** Customer Relationship Management

**CRUD** Create-Read-Update-Delete

**CSA** Cloud Security Alliance

**CSIRT** Computer Security Incident Response Teams

**CSW** Catalog Service for the Web

**DCIFed** DCI Federation Working Group

**DISR** Defense IT Standards Registry

**DMTF** Distributed Management Task Force

**DoD** Department of Defense (USA)

**ebRIM** Electronic business Registry Information Model

**ebXML** Electronic Business using eXtensible Markup Language

**ERP** Enterprise Resource Planning

**EULA** End User License Agreement

**FCCI** Federal Cloud Computing Initiative

**FEA** Federal Enterprise Architecture

**FIPS** Federal Information Processing Standards

**GEIA** Government Electronics & Information Technology Association

**GICTF** Global Inter-Cloud Technology Forum

**GLUE** Grid Laboratory Uniform Environment

**GOTS** Government off-the-shelf

**HTML** HyperText Markup Language

**HTTP** Hypertext Transfer Protocol

**ID-WSF** IDentity Web Service Framework

**I/O** Input/Output

**IaaS** Infrastructure as a Service

IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IODEF	Incident Object Description Format
IP	Internet Protocol
ISIMC	Information Security and Identity Management Committee
ISO	International Organization for Standardization
ISO/IEC JTC 1	International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee 1 Information Technology
IT (ICT)	Information Technology (Note: it is often referred to as ICT [Information and Communications Technologies])
ITU	International Telecommunication Union (The)
ITU-T	ITU Telecommunication Standardization Sector
J2EE	Java 2 Platform, Enterprise Edition
JSON	JavaScript Object Notation
KMIP	Key Management Interoperability Protocol
LDAP	Lightweight Directory Access Protocol
MID	Mobile Internet Devices (USA)
MIL-STDS	Military Standards (USA)
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NIST SP	NIST Special Publication
OAGi	Open Applications Group
OAGIS	Open Applications Group Integration Specification
OASIS	Organization for the Advancement of Structured Information Standards
OAuth	Open Authorization Protocol
OCC	Open Cloud Consortium
OCCI	Open Cloud Computing Interface
ODF	Open Document Format
OGC	Open Geospatial Consortium
OGF	Open Grid Forum
OGSA	Open Grid Services Architecture
OMG	Object Management Group
OOXML	Office Open XML
OS	Operating System
OVF	Open Virtualization Format

P2P	Peer-to-Peer
PaaS	Platform as a Service
PDA	Personal Digital Assistant
PHP	PHP: Hypertext Preprocessor
PI	Personal Information
PII	Personal Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
QoS	Quality of Service
RDF	Resource Description Framework
REST	Representational State Transfer
RSS	Really Simple Syndication
SaaS	Software as a Service
SAJACC	Standards Acceleration to Jumpstart Adoption of Cloud Computing
SAML	Security Assertion Markup Language
SCAP	Security Content Automation Protocol
SDOs	Standards Developing Organizations
SLA	Service Level Agreement
SNIA	Storage Networking Industry Association
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol
SPML	Service Provisioning Markup Language
SSL	Secure Sockets Layer
SSO	Standard Setting Organization
STANAGS	Standardization Agreements
TCG	Trusted Computing Group
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDDI	Universal Description Discovery and Integration
USG	United States Government
VM	Virtual Machine
W3C	World Wide Web Consortium
WG	Working Group
XACML	OASIS eXtensible Access Control Markup Language
XML	Extensible Markup Language

## 15 APPENDIX D – STANDARDS DEVELOPING ORGANIZATIONS

Global Information and Communications Technologies (IT) standards are developed in many venues. Such standards are created through collaborative efforts that have a global reach, are voluntary, and are widely adopted by the marketplace across national borders. These standards are developed not only by national member-based international standards bodies, but also by consortia groups and other organizations.

In July 2009, a Wiki site for cloud computing standards coordination was established: [cloud-standards.org](http://cloud-standards.org). The goal of the site is to document the activities of the various SDOs working on cloud computing standards.

The following is a list of SDOs that have standards projects and standards relevant to cloud computing.

### ATIS

ATIS is accredited by the American National Standards Institute (ANSI). ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of oneM2M, a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications sectors, and a member of the Inter-American Telecommunication Commission (CITEL).

The ATIS Cloud Services Forum (CSF) facilitates the adoption and advancement of cloud services from a network and IT perspective. Drawing upon business use cases that leverage cloud services' potential, the Forum addresses industry priorities and develops implementable solutions for this evolving marketplace. CSF is working to ensure that cloud services – as offered by service providers – are quickly operationalized to facilitate the delivery of interoperable, secure, and managed services. Current priorities include inter-carrier telepresence, content distribution network interconnection, cloud services framework, virtual desktop, virtual private network, and development of a cloud services checklist for onboarding.

### CloudAudit

*CloudAudit* (A6), a working group under the auspices of the CSA (Cloud Security Alliance). Founded in January 2010, *CloudAudit* aims to enable cloud service providers to offer their clients some degree of transparency in an automated, programmatic manner. The group addresses the challenges of lack of transparency and audit requirements in a cloud-based system. The official objective of this working group is to develop a common interface for the automation of the Audit, Assertion, Assessment and Assurance of IaaS (infrastructure as a service), PaaS (platform as a service) and SaaS (software as a service) environments. As of October 2010, *CloudAudit* is officially under the auspices of the Cloud Security Alliance.

## Distributed Management Task Force (DMTF)

DMTF spans the industry with 160 member companies and organizations, and more than 4,000 active participants crossing 43 countries. DMTF members collaborate to develop IT management standards that promote multi-vendor interoperability worldwide.

### Open Virtualization Format (OVF)

#### Open Virtualization Format (OVF) V1.0

OVF 1.1 has been designated as ANSI INCITS 469 2010, and ISO/IEC 17203: 2011.

#### Open Virtualization Format (OVF), OVF 2.0

This specification describes an open, secure, portable, efficient, and extensible format for the packaging and distribution of software to be run in virtual machines. OVF 2.0 includes support for network configuration along with the ability to encrypt the package to ensure safe delivery.

### Open Virtualization Format (OVF)

#### DSP0243 Open Virtualization Format (OVF) V1.1.0

OVF has been designated as ANSI INCITS 469 2010, ISO/IEC 17203:2011.

This specification describes an open, secure, portable, efficient, and extensible format for the packaging and distribution of software to be run in virtual machines.

### Open Cloud Standards Incubator

DMTF's Open Cloud Standards Incubator focused on standardizing interactions between cloud systems by developing cloud management use cases, architectures, and interactions. This work was completed in July 2010. The work has now transitioned to the Cloud Management Working Group.

### Cloud Management Working Group (CMWG)

The CMWG will develop a set of prescriptive specifications that deliver architectural semantics as well as implementation details to achieve interoperable management of clouds between service requestors/developers and providers. This WG will propose a resource model that, at a minimum, captures the key artifacts identified in the use cases and interactions for managing clouds document produced by the Open Cloud Incubator. This group has developed and released the Cloud Infrastructure Management Inter Face (CIMI).

Using the recommendations developed by DMTF's Open Cloud Standards Incubator, the Cloud Management Workgroup (CMWG) is focused on standardizing interactions between cloud systems by developing specifications that deliver architectural semantics and implementation details to achieve interoperable cloud management between service providers and their consumers and developers.

## **Institute of Electrical and Electronic Engineers (IEEE)**

The IEEE Standards Association (IEEE-SA), a globally recognized standards-setting body within the IEEE, develops consensus standards through an open process that engages industry and brings together a broad stakeholder community. IEEE standards set specifications and best practices based on current scientific and technological knowledge. The IEEE-SA has a portfolio of over 900 active standards and more than 500 standards under development.

The IEEE P2301 Working Group (Cloud Profiles) is developing the Guide for Cloud Portability and Interoperability Profiles (CPIP). The guide advises cloud computing ecosystem participants (cloud vendors, service providers, and users) of standards-based choices in areas such as application interfaces, portability interfaces, management interfaces, interoperability interfaces, file formats, and operation conventions.

The IEEE P2302 Working Group (Intercloud) is developing the Standard for Intercloud Interoperability and Federation (SIIF). This standard defines topology, functions, and governance for cloud-to-cloud interoperability and federation.

## **The Internet Engineering Task Force (IETF)**

The Internet Engineering Task Force (IETF) issues the standards and protocols used to protect the Internet and enable global electronic commerce. The IETF develops cyber security standards for the Internet. Current activities include Public Key Infrastructure Using X.509 (PKIX), Internet Protocol Security (IPsec), Transport Layer Security (TLS), Secure Electronic Mail (S/MIME V3), DNS Security Extensions (DNSSEC), and Keying and Authentication for Routing Protocols (karp). Another IETF standard is the Incident Object Description Format (IODEF), which provides a framework for sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incidents. IODEF is an underpinning for the National Information Exchange Model (NIEM), which enables jurisdictions to effectively share critical information on cyber incident management, security configuration management, security vulnerability management, etc.

## **International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee 1 Information Technology (ISO/IEC JTC 1)**

ISO/IEC JTC 1 is the standards development environment where experts come together to develop worldwide Information and Communication Technology (ICT) standards for business and consumer applications. Additionally, JTC 1 provides the standards approval environment for integrating diverse and complex ICT technologies. These standards rely upon the core infrastructure technologies developed by JTC 1 centers of expertise complemented by specifications developed in other organizations. Presently, there are 91 country members. Approximately 2100 technical experts from around the world work within JTC 1. There are presently 18 JTC 1 Subcommittees (SCs) in which most of JTC 1 standards projects are being developed.

JTC 1 SC 27 (IT Security Techniques) is the one JTC 1 SC that is completely focused on cyber security standardization. There are currently three cloud security standards projects in SC27.

ISO/IEC 4th WD 27017, Information security management - Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002 (Technical Specification)  
 Provides organizations using or expecting to use cloud computing services with guidelines for initiating, implementing, maintaining, and improving the information security management based upon ISO/IEC 27002:2005 specific to the cloud computing services.

ISO/IEC 2nd WD 27018, Code of practice for data protection controls for public cloud computing services

Establishes commonly accepted data protection control objectives, controls, and guidelines for implementing controls to meet the requirements identified by a risk assessment. Applies primarily to organizations providing cloud computing services that act as PII processors.

ISO/IEC 1<sup>st</sup> WD 27036-4, Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services

Provides cloud service acquirers and suppliers with guidance on: managing the information security risks caused by using cloud services; integrating information security processes and practices into the cloud –based product and service life cycle processes, while supporting information security controls; responding to risks specific to the acquisition or provision of cloud-based services that can have an information security impact on organisations using these services.

In October 2009, JTC 1 established a new Subcommittee, JTC 1 SC 38 Distributed application platforms and services (DAPS). JTC 1 SC 38 has subsequently established Working Group 3, Cloud computing.

Two Collaborative Teams have been established by ISO/IEC JTC1/SC38/WG3 and ITU-T SG13/WP6:

- Collaborative Team on Cloud Computing Overview and Vocabulary (CT-CCVOCAB)
- Collaborative Team on Cloud Computing Reference Architecture (CT-CCRA).

#### **International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T)**

The ITU-T develops international standards for the telecommunications including voice, data, and video. The primary Study Groups in the ITU-T that are developing standards for cloud computing are SG13: Future networks including cloud computing, mobile and next-generation networks, and SG17: Security.

A new ITU-T Working Party in Study Group 13 (i.e., WP6/13). WP6/13 includes three new Questions or areas of cloud computing study. WP6/13 is currently developing a number of Draft Cloud Computing Recommendation and has established two Collaborative Teams with ISO/IEC JTC 1/SC38. See the JTC 1 SC 38 WG 3 above.

## Kantara Initiative

Kantara Initiative was established on April 20, 2009, by leaders of several foundations and associations working on various aspects of digital identity, aka “the Venn of Identity.” It is intended to be a robust and well-funded focal point for collaboration to address the issues shared across the identity community: Interoperability and Compliance Testing; Identity Assurance; Policy and Legal Issues; Privacy; Ownership and Liability; UX and Usability; Cross-Community Coordination and Collaboration; Education and Outreach; Market Research; Use Cases and Requirements; Harmonization; and Tool Development.

Kantara Initiative is not a standards setting organization for technical specifications. The output of Kantara Initiative is called a Recommendation. Any kind of work can be done in Kantara Initiative but if the work is a technical specification it must be submitted to a standards setting organization upon completion. Other “standards” work such as Operational Frameworks or Usability Guidelines or Interoperability Testing Procedures are the primary focus of Kantara Initiative and will be both developed and maintained by the organization.

## OASIS (Organization for the Advancement of Structured Information Standards)

Founded in 1993, OASIS is a not-for-profit consortium. OASIS develops open standards for the global information society. The consortium produces Eeb services standards along with standards for security, e-business, and standardization efforts in the public sector and for application-specific markets. OASIS has more than 5,000 participants representing over 600 organizations and individual members in 100 countries.

Technical Committees specific to cloud computing include:

Cloud Application Management for Platforms (CAMP) – The purpose of this TC is to define models, mechanisms, and protocols for the management of applications in, and their use of, a Platform as a Service (PaaS) environment.

Cloud Authorization (CloudAuthZ) – The focus of this TC is to develop an interoperable protocol for PaaS (self-service) management interfaces for cloud users to use in developing, deploying and administration of their applications. PaaS management should allow for, but not require, IaaS management to manage the deployment of resources for an application.

Topology and Orchestration Specification for Cloud Applications (TOSCA) – The TC was formed in December, 2011, with the goal to substantially enhance the portability of cloud applications and the IT services that comprise them running on complex virtual and physical software and hardware infrastructure.”

## The Open Cloud Consortium (OCC)

OCC is a member-driven organization that develops reference implementations, benchmarks, and standards for cloud computing. The OCC operates cloud testbeds, such as the Open Cloud Testbed and the OCC Virtual Network Testbed. The OCC also manages cloud computing infrastructure to support scientific research, such as the Open Science Data Cloud.

## Open Grid Forum (OGF)

Open Grid Forum (OGF) is a leading standards developing organization operating in the areas of grid, cloud, and related forms of advanced distributed computing. The OGF community pursues these topics through an open process for development, creation, and promotion of relevant specifications and use cases.

OGF engages partners and participants throughout the international arena to champion architectural blueprints related to cloud and grid computing and the associated specifications to enable the pervasive adoption of advanced distributed computing techniques for business and research worldwide.

Advanced computing built on OGF standards enables organizations to share computing and information resources across department and organizational boundaries in a secure, efficient manner. Organizations throughout the world use production distributed architectures built on these features to collaborate in areas as diverse as scientific research, drug discovery, financial risk analysis, and product design. The capacity and flexibility of distributed computing enables organizations to solve problems that until recently were not feasible to address due to interoperability, portability, security, cost and data-integration constraints.

Cloud systems, grids, and virtualized distributed architectures reduce costs through automation and improved IT resource utilization and improve organizational agility by enabling more efficient business processes. OGF's extensive experience has enabled distributed computing built on these architectures to become a more flexible, efficient, and utility-like global computing infrastructure.

Standardization is the key to realizing the full vision and benefits of distributed computing. The standards developed by OGF enable the diverse resources of today's modern computing environment to be discovered, accessed, allocated, monitored, and managed as interconnected flexible virtual systems, even when provided by different vendors and/or operated by different organizations.

### Open Cloud Computing Interface (OCCI) Working Group

The purpose of this group is the creation of a practical solution to interface with cloud infrastructures exposed as a service (IaaS). The Open Cloud Computing Interface (OCCI) is a RESTful Protocol and API for all kinds of cloud management tasks. OCCI was originally initiated to create a remote management API for IaaS model-based services, allowing for the development of interoperable tools for common tasks including deployment, autonomic scaling, and monitoring. It has since evolved into a flexible API with a strong focus on interoperability while still offering a

high degree of extensibility. The current release of the Open Cloud Computing Interface is suitable to serve many other models in addition to IaaS, including PaaS and SaaS.

### **Object Management Group (OMG)**

The OMG was founded in 1989 and develops standards for enterprise integration. Its membership is international and is open to any organization, both computer industry vendors and software end users. Specific cloud-related specification efforts have only just begun in OMG, focusing on modeling deployment of applications and services on clouds for portability, interoperability, and reuse.

### **Storage Networking Industry Association (SNIA)**

#### **SNIA Cloud TWG**

The SNIA has created the Cloud Storage Technical Work Group for the purpose of developing SNIA Architecture related to system implementations of cloud storage technology. The cloud Storage TWG:

- Acts as the primary technical entity for the SNIA to identify, develop, and coordinate systems standards for cloud storage;
- Produces a comprehensive set of specifications and drives consistency of interface standards and messages across the various cloud storage-related efforts; and
- Documents system-level requirements and shares these with other cloud storage standards organizations under the guidance of the SNIA Technical Council and in cooperation with the SNIA Strategic Alliances Committee.

#### **SNIA Cloud Data Management Interface (CDMI)**

The CDMI specification is now a SNIA Architecture standard and has been submitted to the INCITS organization for ratification as an ANSI and ISO standard as well.

#### **SNIA Terms and Diagrams**

SNIA and OGF have collaborated on cloud storage for a cloud computing white paper. A demo of this architecture has been implemented and shown several times. More information can be found at the Cloud Demo Google Group.

### **Trusted Computing Group (TCG)**

The TCG is a not-for-profit organization formed to develop, define, and promote open, vendor-neutral industry standards for trusted computing building blocks and software interfaces across multiple platforms. TCG has approximately 100 members from across the computing industry, including component vendors, software developers, systems vendors, and network and infrastructure companies.

## **Telecommunications Industry Association (TIA)**

The TIA is accredited by the American National Standards Institute (ANSI) as a standards developing organization (SDO). TIA has created the Cloud Computing Subcommittee (CCSC).

Acting as a liaison between TIA's twelve engineering committees, the CCSC hosts monthly calls open to TIA member companies and engineering committee participants. The focus of these calls is to address ways TIA engineering committees may develop or amend TIA standards pertaining to cloud services. The CCSC also maintains liaison relationships with national and international standards development organizations (SDOs) to determine how existing TIA standards may be adopted to avoid duplication of efforts.

## **TM Forum**

TM Forum is a global, non-profit industry association focused on enabling service provider agility and innovation. As an established thought-leader in service creation, management and delivery, the Forum serves as a unifying force across industries, enabling more than 900 member companies to solve critical business issues through access to a wealth of knowledge, intellectual capital and standards.

The Forum provides a unique, fair, and safe environment for the entire value-chain to collaborate and overcome the barriers to a vibrant, open digital economy, helping member companies of all sizes gain a competitive edge by enabling efficiency and agility in their IT and operations.

TM Forum's Digital Services Initiative focuses on overcoming the end-to-end management challenges of complex digital services, enabling an open, vibrant digital economy. The Forum's work in cloud is targeted at solving the challenges faced by members as they deliver and consume digital services hosted in the cloud.

## **World Wide Web Consortium (W3C)**

Founded in 1994, the W3C is a non-incorporated international community of 334 Member organizations that develop standards in support of web technologies. The W3C work in the area of cyber security standards includes secure transferring data from one domain to another domain or between applications with well-defined document authentication. XML Encryption and XML Signature are key pieces of the XML security stack.

**16 APPENDIX E – CONCEPTUAL MODELS AND ARCHITECTURES****General reference models:**

- Distributed Management Task Force (DMTF): Cloud Service Reference Architecture
- Cloud Computing Use Case Discussion Group: a taxonomy for cloud computing
- IBM: Cloud Reference Architecture
- Cloud Security Alliance: Cloud Reference Model
- Cisco Cloud Reference Architecture Framework
- IETF: Cloud Reference Framework
- ITU-T Focus Group Cloud Reference Architecture

**Reference models focusing on specific application requirements:**

- Open Security Architecture: Secure Architecture Models
- GSA: FCCI (Federal Cloud Computing Initiative)
- Juniper Networks: Cloud-ready Data Center Reference Architecture
- SNIA standard: Cloud Data Management Interface
- Elastra: A Cloud Technology Reference Model for Enterprise Clouds

**17 APPENDIX F - EXAMPLES OF USG CRITERIA FOR SELECTION OF STANDARDS****USG Approach to Selecting Standards****F-1 Analysis Model for Selection of Private Sector Consensus Standards<sup>26</sup>**

NIST has developed a model set of questions to use when evaluating private sector consensus standards for agency use:

## Applicability of standard

- Is it clear who should use the standard and for what applications?
- How does the standard fit into the Federal Enterprise Architecture (FEA)?
- What was done to investigate viable alternative standards (i.e., due diligence) before selecting this standard?

## Availability of standard

- Is the standard published and publicly available?
- Is a copy of the standard free or must it be purchased?
- Are there any licensing requirements for using the standard?

## Completeness of standard

- To what degree does the candidate standard define and cover the key features necessary to support the specific E-Gov functional area or service?

## Implementations on standard

- Does the standard have strong support in the commercial marketplace?
- What commercial products exist for this standard?
- Are there products from different vendors in the market to implement this standard?
- Are there any existing or planned mechanisms to assess conformity of implementations to the standard?

---

<sup>26</sup> <http://www.nist.gov/standardsgov/analysis-model-for-selection-of-consensus-standards.cfm>

#### Interoperability of implementations

- How does this standard provide users the ability to access applications and services through web services?
- What are the existing or planned mechanisms to assess the interoperability of different vendor implementations?

#### Legal considerations

- Are there any patent assertions made to this standard?
- Are there any Intellectual Property Rights (IPR) assertions that will hinder USG distribution of the standard?

#### Maturity of standard

- How technically mature is the standard?
- Is the underlying technology of the standard well-understood (e.g., a reference model is well-defined, appropriate concepts of the technology are in widespread use, the technology may have been in use for many years, a formal mathematical model is defined, etc.)?
- Is the standard based upon technology that has not been well-defined and may be relatively new?

#### Source of standard

- What standards body developed and now maintains this standard?
- Is this standard a de jure or de facto national or international standard?
- Is there an open process for revising or amending this standard?

#### Stability of standard

- How long has this standard been used?
- Is the standard stable (e.g., its technical content is mature)?
- Are major revisions or amendments in progress that will affect backward compatibility with the approved standard?
- When is the estimated completion date for the next version?

## F-2 Department of Defense (DoD)

The DoD IT Standards Registry (DISR) mandates the minimum set of IT standards and guidelines for the acquisition of all DoD systems that produce, use, or exchange information. The Defense Information Systems Agency (DISA) is the executive agent for the DISR. The DISR is updated three times a year.

### Initial Standards Selection Criteria for Inclusion in the DISR

A number of criteria should be considered when evaluating a standard for inclusion in the DISR. Selection criteria include:

- the source of the standard;
- openness;
- technology relevance;
- maturity;
- marketplace support;
- “usefulness/utility”; and
- risk.

Criteria	Description
Source of the Standard	Recognized authority
	Cooperative stance
	Feedback
	Process
	Consensus
Openness	Ownership/IPR
	User Participation
	Vendor Participation
Technology Relevance	
Maturity	Planning Horizon
	Stability
	Revision Content & Schedule
Marketplace Support	Acceptance
	Commercial Viability
Usefulness/Utility	Well-Defined Quality Attributes
	Services & Application Interoperability
Risk	Performance, maturity & stability issues

Table 18 – DoD Selection Criteria and Description Summary

## Standards Source

DoD policy articulates a preference hierarchy based on the source (owner/sponsor/publisher) of the standard. Note that the 5th Priority, Military, has its own internal priority of international first and then DoD MIL-STDs.

The standards preference hierarchy is:

Priority	Standards Source Hierarchy	Example
1 <sup>st</sup>	International	ISO, IEC, ITU
2 <sup>nd</sup>	National	ANSI
3 <sup>rd</sup>	Professional Society; Technology Consortia; Industry Association	IEEE; IETF; W3C; OASIS; GEIA
4 <sup>th</sup>	Government	FIPS
5 <sup>th</sup>	Military	MIL-STDs, STANAGS

Table 19 – DoD Standards Sources Preferences

The standard must be recognized as being available from a reputable and authoritative source. The responsible SDO/Standard Setting Organization (SSO) must have an established position within the relevant technical, professional, and marketplace communities as an objective authority in its sphere of activity. This means that the standard has been created and approved/adopted/published via a formal process and configuration management of the standard has been established. Accreditation implies acceptance by a recognized authoritative SSO.

The Standards Selection Criteria also provides guidance for moving through the standards life cycle that changes the category of a standard from “emerging” to “mandated” to “inactive/retired.”

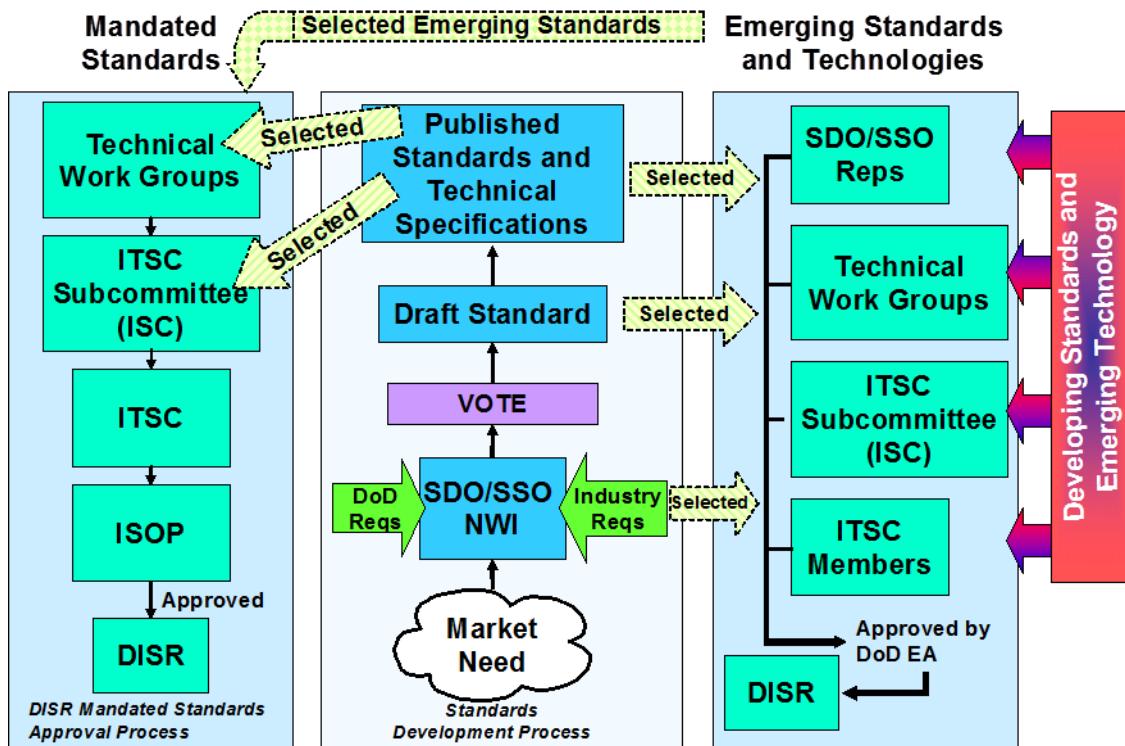


Figure 13 – DoD DISR Standards Selection Process