

Columbia University Cloud Strategy

July 2016

Introduction

Columbia University's adoption of cloud services has increased dramatically, albeit unevenly, across the institution. Given this adoption and the alternative of maintaining on-premise computing capacity, a collective group of Columbia staff has collaborated to provide clear guidelines on how best to utilize the cloud. The guidelines define how to benefit from cloud services in a way that is optimal across the CU enterprise and comports to the University's security and business requirements. A definition of cloud services is included in this document to ensure conformity to a common vocabulary.

Public cloud computing mitigates the risks associated with direct ownership through economies of scale, increased agility, enhanced functionality, resiliency, and flexibility in ways that often complement or replace on-premise hosted servers and services ("private cloud"). The University has already invested significantly in cloud services and we believe that, over the next several years, the increasing availability and advantages of cloud services will result in the elimination of on-premise computing services for all but a small subset of highly specialized services. In this document, we outline a "Cloud First" strategy for Columbia University that transitions CU technology from our traditional on-premise computing model to one employing the public cloud.

What is "The Cloud"?

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.[1] By *public cloud* we mean cloud services provided by service providers (as contrasted with private cloud services that are managed by the institution).

Cloud services are generally categorized into three service models:

Software as a Service (SaaS): The capability for the consumer to use the provider's applications running on a cloud infrastructure. SaaS-based 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 for the consumer to deploy consumer-created or acquired applications developed using programming languages, libraries, services, and supported tools onto a cloud infrastructure, administered by the provider. 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 for the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run their choice of 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).[1]

Why the Public Cloud?

Public cloud services provide a variety of benefits ranging from infrastructure building blocks to full application suites, and benefit from economies of scale through common, integrated solutions that meet the needs of many customers. By offering their products on a global scale, cloud service providers are able to drive efficiency and develop innovative solutions in an unprecedented manner with:

- a. just-in-time capacity provisioning,
- b. built with resiliency and redundancy in mind,
- c. having unparalleled agility, speed and functionality, and
- d. a “pay-as-you-go” cost model.

Cloud First

With publication of this document, Columbia adopts a “Cloud First” strategy for all new IT services, with the anticipation that existing services will be migrated to the public cloud over time as circumstances warrant.

These principles guide the Cloud First strategy:

- University-approved cloud services should be the preferred option for any new service, or when evaluating alternatives or revisions to current services.
- When evaluating applications or platforms, favor those that can be deployed on cloud infrastructure, even if the initial implementation will be run on-premises.
- To avoid “reinventing the wheel,” prefer Software as a Service (SaaS) before Platform (PaaS) or Infrastructure as a Service (IaaS). If a cloud vendor has a service that meets the business need, use it, rather than taking on the cost and effort of using lower service layers to realize the same

or lesser service. SaaS vendors are constantly updating and improving their services at a speed we can never meet.

- While the “SaaS first” approach increases efficiency and enhances capabilities, there is also a risk that must be mitigated: Service providers generally require greater levels of access to University data in order to provide those SaaS services; relatively less data may be need to be exposed to PaaS and IaaS providers. This risk must be mitigated both contractually and technologically.
- Proper procedures must be developed for ensuring the security of University information and complying with all applicable regulations and standards. By developing and applying rigorous data classification and security standards, appropriate technical, legal and financial safeguards can be established.
- Consideration should be given to integration with existing on-premise and other cloud services, including identity management, networking, storage, etc.
- **Columbia University Information Technology and Procurement Services will partner in developing all University-approved cloud service agreements, even in cases where no payment is involved.**

Getting to the Cloud

Deploying new “cloud native” services and migrating existing services to cloud-based solutions will take time and effort. Columbia’s transition strategy consists of:

1. Provisioning of private cloud services managed by CUIT, which are deployed on a converged virtualization infrastructure managed through data centers on the Morningside Heights campus and an alternate data center in Syracuse, NY. Comparable services are offered by CUMC IT and others.
2. Development of automation for IT services configuration and management (“DevOps”) specifically designed for the transition from private to public cloud deployment.
3. Ongoing enhancement of legal, contractual and technical standards to assure compliance with data security and privacy regulations, and University principles.
4. Ongoing assessment, selection and contracting of public cloud providers. Prioritizing which providers are assessed will be determined through a process governed by the IT Leadership Council.
5. Research and development of research computing capabilities that strike an appropriate balance between public-cloud hosted and University-hosted services in the faculty-governed Shared Research Computing Facility at Morningside, and other University research computing facilities.

References

Readers interested in further information in support of this strategy are referred to the following:

- [1] Peter M. Mell and Timothy Grance. 2011. SP 800-145. [The NIST Definition of Cloud Computing](#). Technical Report. NIST, Gaithersburg, MD. *A reference definition of cloud computing, including essential characteristics, service and deployment models.*
- [2] Bedrossian, et. al. 2014. [Cloud Strategy for Higher Education: Building a Common Solution](#). Research Bulletin. EDUCAUSE Center for Applied Research, Louisville, CO. *The basis of our Cloud First strategy, this paper outlines the vision and value of cloud services as well as potential risks and mitigations of using (or of not using) cloud services.*
- [3] Columbia University. 2015. [External Hosting Policy](#). Administrative Policy. Columbia University, New York, NY. *The administrative policy required to be in compliance with University contractual, data security and privacy rules.*