Legislative Council Staff
Nonpartisan Services for Colorado's Legislature

Room 029 State Capitol, Denver, CO 80203-1784
Phone: (303) 866-3521 • Fax: (303) 866-3855
lcs.ga@state.co.us • leg.colorado.gov/lcs

Memorandum

December 15, 2020

TO: Interested Persons

FROM: Jean Billingsley, Senior Research Analyst, 303-866-2357

SUBJECT: Cloud Technical Solutions

Summary

With an ever-growing shift from technical solutions maintained by an organization to using solutions provided by a cloud service provider (CSP), organizations realize several advantages while also discovering the risks associated with cloud solutions. This memorandum will define cloud solutions and summarize the advantages and disadvantages.

Contents

What is the Cloud?

A cloud solution is the provisioning of information technology (IT) capabilities, such as hardware, software, and other technical products and services, to a third-party, known as a CSP. CSPs offer organizations, in both the private- and public-sector, more options in their IT investments. Cloud advantages may include: (1) sharing IT resources with other customers; (2) requesting services to increase or decrease IT resources quickly and on-demand; and (3) pricing models that only charge for IT services requested or used.

Types of Cloud Services

Infrastructure-as-a-Service (IaaS). An IaaS provides servers, networks, storage, and systems to replace the functions of an organization's data center. Some IaaS CSPs also offer telecommunication services, such as using a CSP's infrastructure for a voice-over-IP (VoIP) system. The VoIP IaaS solution might provide communications between physically distant offices as long as an internet connection is available.

Platform-as-a-Service (PaaS). A PaaS maintains server hardware and manages server performance and computing capacity. An organization may install its existing applications and data on the CSP's

servers. Users then access the application via a network connection. New applications may also be developed in a PaaS server. For example, by using PaaS, organizations may develop its custom website and database with the ability to increase or decrease the PaaS capacity along with the corresponding cost.

Software-as-a-Service (SaaS). A SaaS provides all the functions of a traditional application but through a web browser. Examples of a SaaS solution include web-based email services, document applications, customer-resource management applications, and instant messaging.

Other cloud solutions. CSPs also offer a variety of specialized services. Examples of specialized cloud services include:

- Backup-as-a-Service, provides off-site copies of an organization's files, data, or both;
- Disaster Recovery-as-a-Services, provides off-site copies of files, data, configurations, and the applications; and
- Security-as-a-Service, provides some of an organization's cybersecurity functions.

Each cloud solution type might be a:

- public cloud, available to the general public or large industry group;
- private cloud, available only to one organization;
- community cloud, available to a community of users with shared interests; or
- hybrid cloud, consists of two or more private, public, or community clouds.

Cloud Solution Advantages and Disadvantages

The reasons an organization chooses to use cloud solutions may be as simple as having access to a sophisticated data center. Cloud advantages become more apparent for situations requiring a large amount of temporary computing power, both in ease and cost. All the same, an organization may lose control over some critical aspects of its technical solution. The CSP may not only have complete control of the processing and storing of an organization's data but also assumes the responsibility of the performance and maintenance decisions. Equally, compliance and security issues may arise if the organization does not have absolute control of who is viewing or using its data.

In certain instances, an organization's IT department can operate better than a CSP. This is especially true when regulations or contractual obligations prohibit third-party solutions. Furthermore, cloud solutions may present obstacles to the audits that some organizations require. Organizations might also consider the portability of their data from one cloud solution to another. Specifically, an organization may risk losing its data if it procures a new CSP and the prior CSP uses a proprietary file format.

Technical Risks

According to Uptime Institute's 2019 survey, about 70 percent of data center failures are caused by human error.[1] Over half of the survey respondents stated that their downtime incident could have been prevented with better management, processes, or configuration. Although most failures occurred with systems not using the cloud, failures occurring in the cloud accounted for a little over a third of the total reported incidents.

With some cloud solutions, an organization's IT resources will be managing and maintaining the IT components remotely using the CSP's tools. Some cloud solutions require configuration changes to ensure an organization's performance and security requirements are met. At times, the IT staff may need to reconfigure the network connections, the application, and the data storage. Possibly adding even more complexity, most CSPs use different technology and different standards.[2]

Legal Risks

Cloud services not only may cause technical risks, but also legal ones. According to Information Week, the adoption of a cloud solution requires an analysis of the various types of cloud, along with the performance and security requirements.[3] An analysis of the cloud pricing models and subscriptions are also recommended. Gartner Research, an independent technical research firm, explains that cloud sourcing, procurement, and vendor management have some common pitfalls, such as: usage limits, performance, availability, auto-renewal, security, and continuity.[4] CSP contracts may also have ambiguous terms regarding the maintenance of data confidentiality, data integrity, and recovery of data after a data loss incident.

Organizations should also review security breach notification laws and supply chain contract terms. Even if the CSP's security and supply chain provisions are adequate, the reputation of the organization is at risk should a security breach occur. If a CSP does not notify its customers of an incident or security breach, an organization may not be aware of any resulting issues and remediation actions. CSP suppliers may also add risk. A CSP supplier may be listed as one of the restricted vendors maintained by the federal government. For example, a CSP may purchase servers with computer chips from a manufacturing company which was recently added to the federal restricted vendor list because of embedded security vulnerabilities.[5]

---

[1]"How to avoid outages: Try harder!", "Uptime Institute, September 2019, https://journal.uptimeinstitute.com/how-to-avoid-outages-try-harder/, last accessed October 29, 2020.
[2]"Cloud Computing Definitions and Solutions", CIO, https://www.cio.com/article/2424886/cloud-computing-definitions-and-solutions.html?nsdr=true , September 10, 2009, last accessed on October 19, 2020.
[3]"Cloud 101: Getting Started and Saving Costs", InformationWeek, https://www.informationweek.com/cloud/cloud-101-getting-started-and-saving-costs/a/d-id/1338063 , June 19, 2020, last accessed on October 29, 2020.
[4]"SaaS Cloud Contract Management Must Be Strengthened to Reduce Risk and Minimize Unexpected Costs", Gartner Research, https://www.gartner.com/en/documents/3956349/saas-cloud-contract-management-must-be-strengthened-to-r, August 16, 1019, last accessed on October 19, 2020.
[5] "The United States Further Restricts Huawei Access to U.S. Technology", U.S. Department of State, https://www.state.gov/the-united-states-further-restricts-huawei-access-to-u-s-technology/ , last accessed on November 20, 2020.

Cybersecurity and Cloud Technology

While organizations struggle with tight IT budgets and a shortage in the cybersecurity workforce, a cloud solution might be an attractive option. CSP products and services may also be a viable solution when trying to implement critical applications quickly or replace legacy systems that create security vulnerabilities. Even so, according to a 2019 white paper published by the Information Systems Audit and Control Association (ISACA):

- 65 percent of IT professionals underestimate the damage caused by cyberattacks against cloud-based targets;
- only 30 percent of respondents stated that security was primarily the responsibility of the CSP; and
- 20 percent of organizations experienced a cloud incident in 2019.[6]

ISACA further explains that the "absence of policies, standards, and supporting procedures that address security, privacy, and compliance in cloud environments can result in ad-hoc or uninformed assurance activities, which in turn, may conflict with the organization's policies and procedures." Some of the most common challenges, listed in Table 1, are: cloud identity and access management; and cloud network security and encryption.

Table 1
Common Cloud Cybersecurity Challenges

Cloud Identity and Access Management (IAM)	Cloud Network Security and Encryption
Proper IAM enables authorized users or other IT components to access an organization's cloud resources, while also denying access to other individuals.	Encrypting data obfuscates data by converting plain text into a secret code that cannot be decrypted without a key. Data stored in a cloud database should also be encrypted.
An organization's IT resources must learn its CSP's IAM configurations.	Network security and encryption are handled differently with each CSP.
Attackers are aware of potential misconfigurations that present an opportunity.	Some cloud solution's default network configuration settings create vulnerabilities for external threats to exploit.

[6]"Continuous Oversight in the Cloud, How to Improve Cloud Security, Privacy, and Compliance", ISACA, 2019, p. 4.