Staff: Committee on Technology

Irene Byhovsky, Legislative Counsel

Charles Kim, Legislative Policy Analyst

Florentine Kabore, Finance Analyst



##### **THE COUNCIL**

##### **BRIEFING PAPER AND COMMITTEE REPORT OF THE**

##### **INFRASTRUCTURE DIVISION**

*Jeffrey Baker, Legislative Director*

*Terzah Nasser, Deputy Director*

**COMMITTEE ON TECHNOLOGY**

*Hon. Robert Holden, Chairperson*

**December 15, 2020**

**Oversight:**  Benefits and Disadvantages of Cloud-computing Systems

**Preconsidered Int. No. \_\_:** Council Members Torres and Vallone

**Title:** A Local Law in relation to an assessment of the feasibility of storing city agencies' electronic data on cloud computing systems

1. **Introduction**

On December 15, 2020 the Committee on Technology, chaired by Council Member Robert Holden, will hold an oversight hearing on the *Benefits and Disadvantages of Cloud-computing Systems*. The Committee will also hear Preconsidered Int. No. \_\_\_, sponsored by Council Members Torres and Vallone, in relation to an assessment of the feasibility of storing city agencies' electronic data on cloud computing systems. The Committee expects to receive testimony from the Department of Information Technology and Telecommunication (“DOITT”), advocacy groups, academia, and other interested members of the public.

1. **Cloud Computing Systems Background**

Before cloud technology, companies mainly stored their data on hard drives, servers or data centers, situated at their own physical locations.[[1]](#footnote-1) Now, more and more entities take advantage of cloud computing services offered by different providers.[[2]](#footnote-2) These cloud computing service providers allow companies to replace their technological infrastructure with third-party processing and storage capabilities that would then be accessible over the Internet.[[3]](#footnote-3)

“Cloud is a generic term that refers to a network where the physical location and inner workings are abstracted away and unimportant to the usage.”[[4]](#footnote-4) According to the National Institute of Standards and Technology, (“NIST”), a federal laboratory which writes standards for technology, “[c]loud 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.”[[5]](#footnote-5) Harvard University Law Professor Gasser, on another hand, defined cloud computing as “an umbrella term for an emerging trend in which many aspects of computing, such as information processing, collection, storage, and analysis, have transitioned from localized systems (i.e., personal computers and workstations) to shared, remote systems (i.e., servers and infrastructure accessed through the Internet).”[[6]](#footnote-6) Cloud computing is an evolving term with different variations and technologies involved, and therefore, it is not easy to provide a strict and standardized definition.[[7]](#footnote-7)

Before examining the in-depth advantages and risks associated with cloud computing systems it is necessary to understand different types of cloud service and deployment models.

1. **Types of Cloud Computing Service Models**

There are presently three types of service models of cloud computing systems: Software as a Service (“SaaS”), Platform as a Service (“PaaS”), and Infrastructure as a Service (“IaaS”).[[8]](#footnote-8)

SaaS is “a complete software solution that users purchase on a pay-as-you-go basis from a cloud service provider.”[[9]](#footnote-9) It allows users from different locations to use it without actually installing the software or applications on their devices.[[10]](#footnote-10) These applications can be accessed from a web browser, like web-based email, or a program interface. The cloud computing consumer does not have any control over the underling cloud infrastructure like the network, servers, storage, or even the individual application’s capabilities, with the possible exception of limited control over the application’s configuration settings specific to the user.[[11]](#footnote-11) All of the underlying infrastructure, middleware, software and data are located in the service provider’s data center.[[12]](#footnote-12) The service provider manages the hardware and software, and sometimes ensures the availability and the security of the app and data.[[13]](#footnote-13) For example, Google utilizes this SaaS model to deliver its popular application Google Docs, where the user accesses Google’s software by signing in to their Google account through their web browser and can then use the Google Docs word processor, no software installation required.[[14]](#footnote-14)

PaaS provides the consumer with the platform and tools to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.[[15]](#footnote-15) While the consumer of these services does not control or manage the underlying cloud infrastructure like the network, servers, or storage, they have control over the applications deployed through this cloud infrastructure as well as, in some cases, the configuration settings for the environment in which their applications would be implemented.[[16]](#footnote-16) Examples include Microsoft Azure App Services and Google App Engine, where developers can build their own applications and services more quickly and efficiently by using these platforms to bypass development hurdles like managing application infrastructure and software licenses.[[17]](#footnote-17) For instance, the hugely popular educational nonprofit Khan Academy uses Google App Engine to develop and host its online applications, enabling the organization to stop worrying about deployment issues and running servers and instead focus full-time on developing content and the user experience.[[18]](#footnote-18)

IaaS provides the consumer with computing resources like processing, storage, and networks, and other fundamental resources where the consumer can deploy and run arbitrary software such as operating systems and applications.[[19]](#footnote-19) The cloud computing consumer does not manage or control the underlying cloud infrastructure, but can control elements like the operating systems, storage, and deployed applications, in addition to possible limited control of select networking components like hosting firewalls.[[20]](#footnote-20) It, among other things, enables its users to store files on remote cloud servers and share files in a synchronized way.[[21]](#footnote-21) One of the most prominent examples of IaaS is Amazon Web Services, specifically as Netflix uses Amazon Web Services to host all of its IT operations and for most of its computing and storage needs.

1. **Types of Deployment Models**

According to NIST, there are four basic deployment models: Private cloud, Community cloud, Public cloud and Hybrid cloud.

**Private cloud**. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

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

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

**Hybrid cloud**. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).[[22]](#footnote-22)

The advent of cloud computing has significantly impacted how information is collected, stored, and distributed by all entities, from individuals to businesses and government agencies. And while the development and adoption of cloud computing has rapidly expanded, cloud computing brings both benefits and risks.[[23]](#footnote-23)

1. **Benefits of Cloud Computing Systems**

Cloud computing services may provide some savings on overhead and infrastructure costs as well as permit easy access over the Internet or over a network from any location, so that computer software and data may be readily available.[[24]](#footnote-24)  Additionally, migrating to the cloud can provide a number of improvements for companies and businesses, including: a faster and more adaptable network and business operations that can more easily accommodate changes like upgrades and increased technological demands; easier management of increasing resource demands; better consumption management of the cloud resource; and overall improved performance.[[25]](#footnote-25)

The major benefits of using cloud computing technology are accessibility and possible low operation cost. With cloud computing, consumers benefit from increased accessibility to data applications, software, and other IT resources, as they can access software and applications, stored data, processing and network capabilities, and other fundamental computing resources from anywhere in the world.[[26]](#footnote-26) A cloud computing consumer may obtain substantial cost savings primarily because they do not have to maintain their own IT infrastructure and can therefore avoiding the substantial upfront costs that come with it, like the purchase and installation of computer hardware, software licensing costs, and the high yearly costs that would come with regular upgrades, maintenance, and system administration.[[27]](#footnote-27) Instead, the company uses the cloud service provider's infrastructure, and the service provider takes care of managing any upgrades, maintenance, and system administration in the cloud.[[28]](#footnote-28)

1. **Risks Associated with Cloud Computing Systems**

Cloud computing services have potential value, but it is also important to recognize its potential risks, such as risks are related to cost, security, and reliable broadband access.

The first factor that some businesses might consider before switching to cloud computing services is related to costs. With cloud computing, a business does not have to purchase or install its own servers or other extra equipment, however, there are “up-front” costs associated with a transition to cloud computing, such as training employees to use the system.[[29]](#footnote-29) Moreover, “findings from the past two Enterprise Cloud Index (“ECI”) surveys,” commissioned by cloud computing company Nutanix, “show that about 35% of businesses using public cloud services are over budget. In addition, these studies repeatedly find that, on average, as much as 35% of public cloud spend is going to waste because companies choose the wrong service or pricing plan, or leave resources idle or forgotten, racking up unwanted charges each month.”[[30]](#footnote-30) While initially, the public cloud may be less expensive, over time, it starts to lose its value.[[31]](#footnote-31) In other words, while the cost of cloud computing services is lower in the first year because of the costs saved from installation and purchase of an IT infrastructure, it usually is more expensive in the long-run relative to their client/server counterparts. However, as a cloud computing business never stops paying for services, it will likely end up costing more over the life of their use of the platform.[[32]](#footnote-32)

The next factor is security.[[33]](#footnote-33) The cloud computing model is far from universally trusted due to the fact that sensitive data is leaving the premises and control of their owners.[[34]](#footnote-34) In our age where hacking is an ever-present danger, this is a foremost concern for industries that interact with and manage highly sensitive information.[[35]](#footnote-35) There are a number of ways in which hackers can attack the cloud, such as phishing, which seeks information under false pretenses using email or other online channels; fraud; and the exploitation of software to take over users’ accounts, gaining control which gives hackers the same visibility and control of the cloud services as the users themselves.[[36]](#footnote-36) There are also distributed denial of service attacks, also known as “DDoS” attacks, which entail attackers flooding online webpages or services with so much traffic so as to forcibly crash the back-end systems under the sheer weight and volume of the online traffic.[[37]](#footnote-37) DDoS attacks may allow hackers to “extort service providers,” that is, crucially, the cloud provider companies themselves, “for significant amount of dollars with mere threats of such an attack.”[[38]](#footnote-38)

Stricter laws about where customer data can be stored have also forced IT leaders to rethink where their existing workloads are allowed to run. [[39]](#footnote-39) Nearly three-quarters **(73%)** of respondents to the Second Annual ECI study in 2019, brought some applications and data back from public clouds to on-premise environments, meaning respondents moved data from offsite public cloud infrastructure to their own onsite IT infrastructure.[[40]](#footnote-40)Among the reasons provided were security concerns created by new and emerging privacy laws, such as Europe’s General Data Protection Regulation (“GDPR”). Since then, other global privacy legislation based on GDPR has been forcing companies to carefully orchestrate where they store customer information and to build processes that ensure they have instant access to that information, should requests for it present themselves.[[41]](#footnote-41) Moreover, cloud computing providers may have servers outside the United States, and, if so, may be subject to the laws of a foreign jurisdiction and, possibly, the victim of international political strife.[[42]](#footnote-42) According to ECI research, security and compliance remain top of mind for enterprises deciding what infrastructure models to deploy.[[43]](#footnote-43)

Other factors that also introduce potential risks are mandatory Internet connectivity,[[44]](#footnote-44) the financial stability of a cloud computing provider, the long-term expenses, the physical location of a data center, the cost of moving or removing the data[[45]](#footnote-45) and other factors.

1. **Cloud Computing Systems in New York City**

In 2017, the Department of Information Technology and Telecommunications (“DoITT”) issued the Citywide Policy on Cloud Services (“Citywide Policy”).[[46]](#footnote-46) The Citywide Policy addresses the main issues related to migrating data to cloud computing systems, including cybersecurity, Internet connectivity, as well as essential considerations for cloud service agreements. Those considerations include, among other things: backup policy, data retention, portability, data ownership, data commingling, encryption, cybersecurity incidents, penetration testing and vulnerability scans.[[47]](#footnote-47)

According to the Citywide Policy, “[a]ll City uses of IaaS must be managed through DoITT’s Self Provisioning Gateway (“SPG”). For IaaS cloud services not yet available through the SPG, City entities must submit their implementation plan to DoITT to determine the best approach and ensure information security. The SPG is a web portal for New York City agencies to obtain secure provisioning of cloud infrastructure. The SPG enables authorized administrators, developers, or business users to self-provision select classes of virtual machines in DoITT’s ‘private cloud’ or in select external cloud service providers, as they become available. Virtual machines are quickly provisioned through automation. The user of the SPG is then able to use, maintain, and operate their virtual machines throughout the virtual machine’s entire lifecycle.” [[48]](#footnote-48)

With regard to SaaS and PaaS, “[a]ll City uses of SaaS or PaaS must be reviewed and approved by Citywide Cybersecurity prior to procurement and implementation. City entities are advised to inform DoITT of their plans to leverage a SaaS or PaaS solution as soon as they have chosen the product, but at the very least, before a contract is signed. DoITT’s technical team will review critical aspects of the SaaS or PaaS solution.” [[49]](#footnote-49)

* 1. **City Agencies Using Cloud Computing Systems**

There are many New York City agencies utilizing cloud computing systems for their operations. Notably, the New York City Department of Transportation used the cloud to build and host its web applications Vision Zero View and iRide NYC.[[50]](#footnote-50) Additionally, the New York Public Library has used cloud computing systems to build and host its primary website and digital-collections website, as well as reinforce its online security infrastructure.[[51]](#footnote-51) The New York City Department of Youth and Community Development (“DYCD”) used the cloud to build a web app called discoverDYCD, an online platform that allows users to find information on the availability of certain opportunities and programs, in addition to offering a simplified application process between programs.[[52]](#footnote-52) Further, New York City Cyber Command developed a cloud infrastructure with third parties to help its cybersecurity experts detect and react to threats faster.[[53]](#footnote-53)

1. **Legislative Analysis of Preconsiderd Int. No. \_\_\_**

Preconsidered Int. No. \_\_\_\_ would require the Department of Information Technology and Telecommunications to conduct an assessment of the feasibility of transferring city agencies’ electronic data to cloud computing systems. The assessment would include, but not be limited to: an analysis of the feasibility of transitioning legacy systems to utilize the cloud; an analysis of any implications related to current software licenses; an estimate of the costs, per unit of data, of storing, retrieving, and removing data from the average cloud computing system. It would also include recommendations on the requirements that a prospective cloud computing service provider should meet, such as on the physical data center location, the physical security of the data center, the disaster recovery strategy, the mechanics of reporting a security breach, the level of encryption, the financial stability of the provider, suggested auditing protocols, and the inclusion of an indemnification clause in any contract. The Department would also be required to submit a report of the results of the assessment to the Council.

The local law would take effect immediately.

1. **Conclusion**

The Committee looks forward to receiving testimony from the Administration, advocacy groups, academia, and other interested members of the public on the operation of city agencies and whether they can operate more effectively and cost-efficiently by utilizing cloud computing services.

Preconsidered Int. No.

By Council Members Torres and Vallone

..title

A Local Law in relation to an assessment of the feasibility of storing city agencies’ electronic data on cloud computing systems

..Body

Be it enacted by the Council as follows:

Section 1. Assessment of the feasibility of storing city agencies’ electronic data on cloud computing systems.

a. Definitions. For the purposes of this section, the term “department” means the department of information technology and telecommunications.

b. The department shall conduct an assessment to determine the feasibility of storing city agency electronic data at rest on cloud computing systems, rather than on physical data storage systems owned by the city.

c. No later than September 1, 2021, the department shall submit to the speaker of the council a report of the results of the assessment conducted pursuant to subdivision b of this section. Such report shall include, but not be limited to, the following:

1. an establishment of data classification categories for use with cloud computing services, including an inventory of the various data types;

2. an analysis of the feasibility and security of storing data from each data classification category on the cloud, including the legal implications, if any;

3. an analysis of the feasibility of transitioning legacy systems to utilize the cloud;

4. an analysis of any implications related to current software licenses;

5. an estimate of the costs, per unit of data, of storing, retrieving, and removing data from the average cloud computing system;

6. potential cost differentials, in both personal services and other than personal services costs, between physical data storage and cloud storage;

7. a brief analysis of the prospective cloud computing service providers, including a description of their physical principal places of business; and

8. recommendations on the requirements that a prospective cloud computing service provider should meet, such as on the physical data center location, the physical security of the data center, the deployment model of the cloud computing system, the disaster recovery strategy, the mechanics of reporting a security breach, the data duplication process utilized, the level of encryption utilized, the financial stability of the provider, the auto-deletion options, suggested auditing protocols, and any terms that a contract with a cloud computing service provider should include, such as an indemnification clause.

§ 2. This local law takes effect immediately.

IB

LS #13515; 15719

09/29/2020

1. Susan Moore, *Gartner Says a Massive Shift to Hybrid Infrastructure Services is Underway,* Gartner, Inc., April 5, 2017, <https://www.gartner.com/en/newsroom/press-releases/2017-04-05-gartner-says-a-massive-shift-to-hybrid-infrastructure-services-is-underway>. [↑](#footnote-ref-1)
2. *See* Smith, *Electronic Discovery: The Challenges of Reaching Into the Cloud*, 52 Santa Clara L Rev, at 1561, 1562 (2012). [↑](#footnote-ref-2)
3. Smith, *Electronic Discovery: The Challenges of Reaching Into the Cloud*, 52 Santa Clara L Rev, at 1561, 1562 (2012) (citing Mark L. Austrian & W. Michael Ryan, Cloud Computing Meets EDiscovery, CYBERSPACE LAW., July 2009, at 1) [↑](#footnote-ref-3)
4. Josiah Dykstra, *Forensic Collection of Electronic Evidence from Infrastructure –as-a- Service Cloud Computing,* 19 Rich. J. L. &Tech. 1, 7 (2012). [↑](#footnote-ref-4)
5. [Evelyn Brown](mailto:evelyn.brown@nist.gov), *Final Version of NIST Cloud Computing Definition Published*, **NIST** Tech Beat. (Oct., 2011), <http://www.nist.gov/itl/csd/cloud-102511.cfm>. [↑](#footnote-ref-5)
6. Urs Gasser et al., *Internet Monitor 2013: Reflections on the Digital World*, BERKMAN CTR FOR INTERNET & SOC'Y 1, 25, (2013); *see* also Dr. George Yijun Tian, *Cloud Computing and Cross-Border Transfer Pricing: Implications of Recent Oecd and Australian Transfer Pricing Laws on Cloud Related Multinational Enterprises and Possible Solutions*, 44 Rutgers Computer & Tech LJ 33, 91 [2018]. [↑](#footnote-ref-6)
7. *See* Dr. George Yijun Tian, *Cloud Computing and Cross-Border Transfer Pricing: Implications of Recent OECD and Australian Transfer Pricing Laws on Cloud Related Multinational Enterprises and Possible Solutions*, 44 Rutgers Computer & Tech LJ 33, 91 [2018]. [↑](#footnote-ref-7)
8. *The NIST Definition of Cloud Computing*, NIST, Special Publication 800-145, <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>. [↑](#footnote-ref-8)
9. See What is SaaS?, MICROSOFT AZURE, <https://azure.microsoft.com/en-au/overview/what-is-saas/>. [↑](#footnote-ref-9)
10. *See Id*. [↑](#footnote-ref-10)
11. *The NIST Definition of Cloud Computing*, NIST, Special Publication 800-145. [↑](#footnote-ref-11)
12. See What is SaaS?, MICROSOFT AZURE, <https://azure.microsoft.com/en-au/overview/what-is-saas/>. [↑](#footnote-ref-12)
13. See id. [↑](#footnote-ref-13)
14. *What can you do with Docs?*, Google Workspace Learning Center, <https://support.google.com/a/users/answer/9300503?hl=en>. [↑](#footnote-ref-14)
15. *See* *The NIST Definition of Cloud Computing*, NIST, Special Publication 800-145. [↑](#footnote-ref-15)
16. *Id*. [↑](#footnote-ref-16)
17. *See* *What is PaaS?,* Microsoft Azure, <https://azure.microsoft.com/en-us/overview/what-is-paas/>. [↑](#footnote-ref-17)
18. Google Cloud, *Khan Academy: Scaling and Simplifying*, Google Cloud, <https://cloud.google.com/customers/khan-academy>. [↑](#footnote-ref-18)
19. *The NIST Definition of Cloud Computing,* NIST, Special Publication 800-145. [↑](#footnote-ref-19)
20. *Id*. [↑](#footnote-ref-20)
21. *See* Dr. George Yijun Tian, *Cloud Computing and Cross-Border Transfer Pricing: Implications of Recent OECD and Australian Transfer Pricing Laws on Cloud Related Multinational Enterprises and Possible Solutions*, 44 Rutgers Computer & Tech LJ 33, 44 [2018]. [↑](#footnote-ref-21)
22. The NIST Definition of Cloud Computing, NIST, Special Publication 800-145 (emphasis added). [↑](#footnote-ref-22)
23. Dr. George Yijun Tian, *Cloud Computing and Cross-Border Transfer Pricing: Implications of Recent Oecd and Australian Transfer Pricing Laws on Cloud Related Multinational Enterprises and Possible Solutions*, 44 Rutgers Computer & Tech LJ 33, 35 [2018]. [↑](#footnote-ref-23)
24. . *See* W. Michael Ryan & Cristopher M. Loeffler, *Insights into* *Cloud Computing*, 22 Intell. Prop.& Tech. L.J. 22, 22 (2010). [↑](#footnote-ref-24)
25. Cloud Migration, Accenture, <https://www.accenture.com/us-en/insights/cloud-migration-index>. [↑](#footnote-ref-25)
26. *See* Ryan & Loeffler, *Insights into* *Cloud Computing*, *supra* note at 22; *see also* Orly Mazur, *Taxing the Cloud*, 103 Calif. L. Rev. 1, 9 (2015). [↑](#footnote-ref-26)
27. *See* Orly Mazur, *Taxing the Cloud*, 103 Calif. L. Rev. 1, 9 (2015). [↑](#footnote-ref-27)
28. *See* Orly Mazur, *Taxing the Cloud*, 103 Calif. L. Rev. 1, 9 (2015). [↑](#footnote-ref-28)
29. *See* Tim Maurer & Garrett Hinck, *Cloud Security: A Primer for Policymakers*, Carnegie Endowment for International Peace, Aug 31, 2020, <https://carnegieendowment.org/2020/08/31/cloud-security-primer-for-policymakers-pub-82597>. [↑](#footnote-ref-29)
30. Kenzie Pittman*, Why Businesses Move Apps Out of the Public Cloud,* Nutanix, Inc*, March 24, 2020,* [*https://www.nutanix.com/theforecastbynutanix/business/why-businesses-are-moving-apps-out-of-the-public-cloud*](https://www.nutanix.com/theforecastbynutanix/business/why-businesses-are-moving-apps-out-of-the-public-cloud)*.* (citing Ryan Arnold, IT director at Acumen, LLC). [↑](#footnote-ref-30)
31. *Id.* [↑](#footnote-ref-31)
32. Tim Maurer & Garrett Hinck, *Cloud Security: A Primer for Policymakers*, Carnegie Endowment for International Peace, Aug 31, 2020, <https://carnegieendowment.org/2020/08/31/cloud-security-primer-for-policymakers-pub-82597>. [↑](#footnote-ref-32)
33. Kenzie Pittman*, Why Businesses Move Apps Out of the Public Cloud, Nutanix, Inc,* March 24, 2020, <https://www.nutanix.com/theforecastbynutanix/business/why-businesses-are-moving-apps-out-of-the-public-cloud>*.* [↑](#footnote-ref-33)
34. *See* Nina Lukina, *Is the Cloud Safe for Law Firms? Addressing Common Concerns about Privacy, Compliance, and Connectivity*, NY St BJ, May 2018, at 52. [↑](#footnote-ref-34)
35. *See* Nina Lukina, *Is the Cloud Safe for Law Firms? Addressing Common Concerns about Privacy, Compliance, and Connectivity*, NY St BJ, May 2018, at 52. [↑](#footnote-ref-35)
36. J. Nicholas Hoover, *Compliance in the Ether: Cloud Computing, Data Security and Business Regulation*, 8 J Bus & Tech L 255, 261-62 [2013] (citing Cloud Sec. Alliance, Top Threats to Cloud Computing 14 (2010)), <https://ioactive.com/wp-content/uploads/2018/05/csathreats.v1.0-1.pdf>. [↑](#footnote-ref-36)
37. *Id.* [↑](#footnote-ref-37)
38. *Id*. [↑](#footnote-ref-38)
39. # For example, in 2019, nearly three-fourths of ECI respondents **(73%)** reported having brought some public cloud applications back on-prem, and of those **22%** reported moving five or more applications. Wendy M. Pfeiffer, *Third Annual ECI Report: How the Pandemic Raised IT’s Profile and Paved a Clearer Pathway to Hybrid Cloud*, Nutanix, <https://www.nutanix.com/blog/third-annual-enterprise-cloud-index-report>; Vanson Bourne, Nutanix Enterprise Cloud Index 2019 Edition, Nutanix, <https://www.nutanix.com/content/dam/nutanix/resources/gated/analyst-reports/enterprise-cloud-index-2019.pdf>.

    [↑](#footnote-ref-39)
40. *Id*. [↑](#footnote-ref-40)
41. *Id*. [↑](#footnote-ref-41)
42. Tim Maurer & Garrett Hinck, *Cloud Security: A Primer for Policymakers*, Carnegie Endowment for International Peace, Aug 31, 2020, <https://carnegieendowment.org/2020/08/31/cloud-security-primer-for-policymakers-pub-82597>. [↑](#footnote-ref-42)
43. *Id.* [↑](#footnote-ref-43)
44. If Internet connection goes down or is not reliable, there will be no connection to the system. As time progresses, Internet connection disruptions are becoming more and more rare. Thus, going forward, this may not be a disadvantage. [↑](#footnote-ref-44)
45. Tim Maurer & Garrett Hinck, *Cloud Security: A Primer for Policymakers*, Carnegie Endowment for International Peace, Aug 31, 2020, <https://carnegieendowment.org/2020/08/31/cloud-security-primer-for-policymakers-pub-82597>. [↑](#footnote-ref-45)
46. *Citywide Cloud Policy*, NYC DOITT, February 23, 2017, <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjN2bX8nMTtAhWEMd8KHV57BFkQFjABegQIAhAC&url=http%3A%2F%2Fwww.bidnet.com%2Fbneattachments%3F%2F444886615.pdf&usg=AOvVaw25844KZWvTB75nW1N5WDB3>. [↑](#footnote-ref-46)
47. *See id* (Appendix 1). [↑](#footnote-ref-47)
48. *Citywide Cloud Policy*, NYC DOITT, February 23, 2017. [↑](#footnote-ref-48)
49. *Id*. [↑](#footnote-ref-49)
50. *AWS Case Study: New York City Department of Transportation*, Amazon Web Services, <https://aws.amazon.com/solutions/case-studies/nyc-dot/>. [↑](#footnote-ref-50)
51. *New York Public Library Case Study*, Amazon Web Services, 2016, <https://aws.amazon.com/solutions/case-studies/new-york-public-library/>. [↑](#footnote-ref-51)
52. *Fulfilling consistent societal needs with cloud technology at NYC DYCD*, Microsoft Azure, 2020, <https://customers.microsoft.com/en-us/story/839880-new-york-city-government-azure-en-unitedstates>. [↑](#footnote-ref-52)
53. *NYC Cyber Command: Keeping New York City’s digital services more secure at massive scale,* Google Cloud, <https://cloud.google.com/customers/nyc-cyber-command>. [↑](#footnote-ref-53)