New Jersey Office of Information Technology

February 20, 2020

IT Circular

Enterprise Cloud Computing Guidelines

20-01-NJOIT

PURPOSE

The New Jersey Office of Information Technology (NJOIT) recognizes the value of public cloud computing to enhance service delivery and improve operational efficiencies for the State of New Jersey. The goal of this circular is to outline NJOIT's strategy to adopt public cloud computing and how it will facilitate diverse uses of public cloud computing, while ensuring optimal levels of technology services and security.

This circular outlines the considerations that must be addressed when using public cloud computing. This is not a comprehensive review of all considerations, so Agencies must be aware of the due diligence that they must exercise in exploring public cloud computing options. NJOIT serves as an enterprise resource in this regard and will provide details about the provisioning process for third-party public cloud solutions used by NJOIT and other Executive Branch Agencies. NJOIT can provide Agencies with assistance in identifying legacy applications and workloads that could benefit from public cloud integration, optimization, or re-platforming/re-architecting with guidance on procurement and application development methodologies.

Agencies within the Executive Branch of government in the State of New Jersey should leverage public cloud computing that will reduce information technology costs while maximizing availability, integrity, confidentiality and interoperability of State data, applications, and IT infrastructure. Business requirements must drive the public cloud computing decision making process. Public cloud computing should be adopted where it is cost effective, meets system/owner mission requirements, and provides the required levels of security and performance.

Public cloud computing procurement, account and subscription provisioning, and high-level management will be centralized through NJOIT in order to ensure the standardization of security controls and base-line compliance with the latest publication of the Statewide Information Security Manual (SISM). Aggregation through NJOIT is also consistent with Executive Order 225 (Christie 2017), to standardize and consolidate computing infrastructure. Finally, centralization of cloud computing procurement and provisioning reduces cloud sprawl

and "shadow IT." Compliance with this circular ensures all uses of public cloud computing meet the State's security, performance, technical, and administrative requirements.

NJOIT'S ENTERPRISE CLOUD STRATEGY

NJOIT's initial enterprise cloud strategy is to focus first on cloud infrastructure as a service (IaaS) and cloud platform as a service (PaaS) computing efforts on low and moderate sensitivity workloads. DevOps, development, and testing environments are good initial candidates for integration into public cloud computing, as are low-risk data archive and backup workloads. Furthermore, projects hosting public data are well suited for initial public cloud computing efforts, as are "value add" modules or components that can integrate with existing applications or systems, thereby immediately adding value or functionality. Over time, NJOIT anticipates expanding the range and scope of applications appropriate for public cloud computing based on the operational maturity of the solutions, cost, security, availability, and compliance requirements. This phased strategy will drive better business outcomes, including higher returns on investment, agility, and service level agreement metrics.

There are four (4) key factors for identifying workloads appropriate for migration or initiation into public cloud computing: data classification, application performance factors, the cloud-readiness of the application, and cost.

1. Data Classification and Workloads

First, the SISM requires assets and information be classified according to their sensitivity and criticality; specifically, SISM, SC-01: Security Categorization, (Systems inherit the highest categorization for the information which they generate, store, process, or transmit) and SISM, SC-03: Assigning Security Categorizations. For additional information on data classification, please refer to the New Jersey Data Classification Schema and Guidelines.

Workloads categorized as low-impact and involving data classified as either "public" or "internal use" are a best fit for public cloud computing, as compared moderate or high impact workloads which typically involve data that is classified as either "confidential" or "restricted." Workloads classified as low-impact that suffer a loss of confidentiality, integrity, or availability present a limited adverse effect on organization operations, organizational assets, individuals, other organizations, or the State of New Jersey. In contrast, medium- and high- impact workloads that suffer a loss of confidentiality, integrity, or availability will present either a significant or severe degradation on organization operations, organizational assets, individuals, other organizations, or the State of New Jersey. This is because moderate- and high- impact workloads require control and customization of the underlying information technology infrastructure to ensure confidentiality, integrity, and availability, thus making them less appropriate for public cloud computing. While it may be possible to architect a public cloud computing solution to mitigate the risks of moderate and high impact workloads,

the time-to-market and costs associated may be substantial, thus weakening the business case factors driving the consideration of public cloud computing.

If public cloud computing risks can be mitigated, or when the agility and flexibility of public cloud computing resources outweigh the risks, moderate or high workload classified systems can benefit from public cloud computing integration. For instance, specific cloud architecture designs, encryption techniques, and "government cloud" offerings[1] may sufficiently reduce potential impacts, thus allowing moderate and high impact workloads to benefit from public cloud computing.

2. Performance Tolerance

Workloads that require high performance virtual machines, significant bandwidth and high data transfer or upload/download functionality, and very-low latency tolerance are generally not good candidates for public cloud computing. In general, public cloud computing costs are a combination of an hourly rate charged depending on the size of the virtual machine, plus network connection costs, and storage costs. Therefore, large performance-oriented virtual machines are expensive to operate, due to their reserved computing power and anticipated data inputs and outputs. Similarly, applications with large, recurring data uploads and downloads between the State and the public cloud may increase burdens on the Garden State Network (GSN) and result in increased input/output (I/O) costs charged by the cloud service provider.

Agencies should also consider the application's points of integration, both on premises and inter-cloud. With increased integration requirements, costs and complexity also increase, making public cloud computing a less suitable solution. As with the data security classification, it is possible to architect a cloud solution to mitigate risks posed by performance and latency degradation; however, these efforts increase the costs and complexity of public cloud computing and may negate the benefits and attractiveness of public cloud computing.

3. Cloud Readiness

Because public cloud computing resources are billed based on resources consumed, the "lift-and-shift" migration of large, monolithic legacy applications to public cloud computing would likely result in increased operational costs, as compared to on-premises hosting. Many applications would require some degree of re-factoring, re-architecting, re-engineering, re-platforming, or right-sizing in order to fully leverage the benefits of the public cloud computing

---

[1] Commercial vs. Government Clouds – NJOIT's current public cloud subscriptions are for commercial cloud offerings. Specialized data governance needs drive the decision making on commercial versus government cloud adoption, e.g. compliance with FBI Criminal Justice Information Services Division (CJIS).

environment. Accordingly, new application builds or applications that are already containerized and leverage virtualized components would be good candidates for public cloud computing, as would be applications that only require minor platform upgrades or modifications. In contrast, large monolithic applications with heavy integration points must be closely scrutinized in order to determine if it is even possible to migrate the application to the cloud, or if modifications to the application would allow the application to operate efficiently within a cloud model. For example, high integration or connectivity needs weigh against a public cloud model. Applications that require low latency, offline execution, or interaction with other State systems are not good candidates for public cloud migration. Applications with these attributes generally incur increased costs to meet these business requirements that could be avoided with on-premises hosting.

4. Cost

Public cloud computing resources provide agility, responsiveness, and cost savings, but may interject potential security issues, vendor lock-in issues, integration challenges, and regulatory challenges. After considering the three major factors, Agencies should attempt to determine whether or not the costs to be incurred by migrating to the public cloud are predictable and reasonable, whether or not all other risks can be tolerated or appropriately mitigated and whether or not public cloud attributes are either benefits or risks to the application.

Agencies should compare costs across multiple Cloud Service Providers. Depending on the workload and licensing requirements, initial migration and ongoing operating costs may vary widely.

The following decision tree depicts the cloud readiness approach described above:

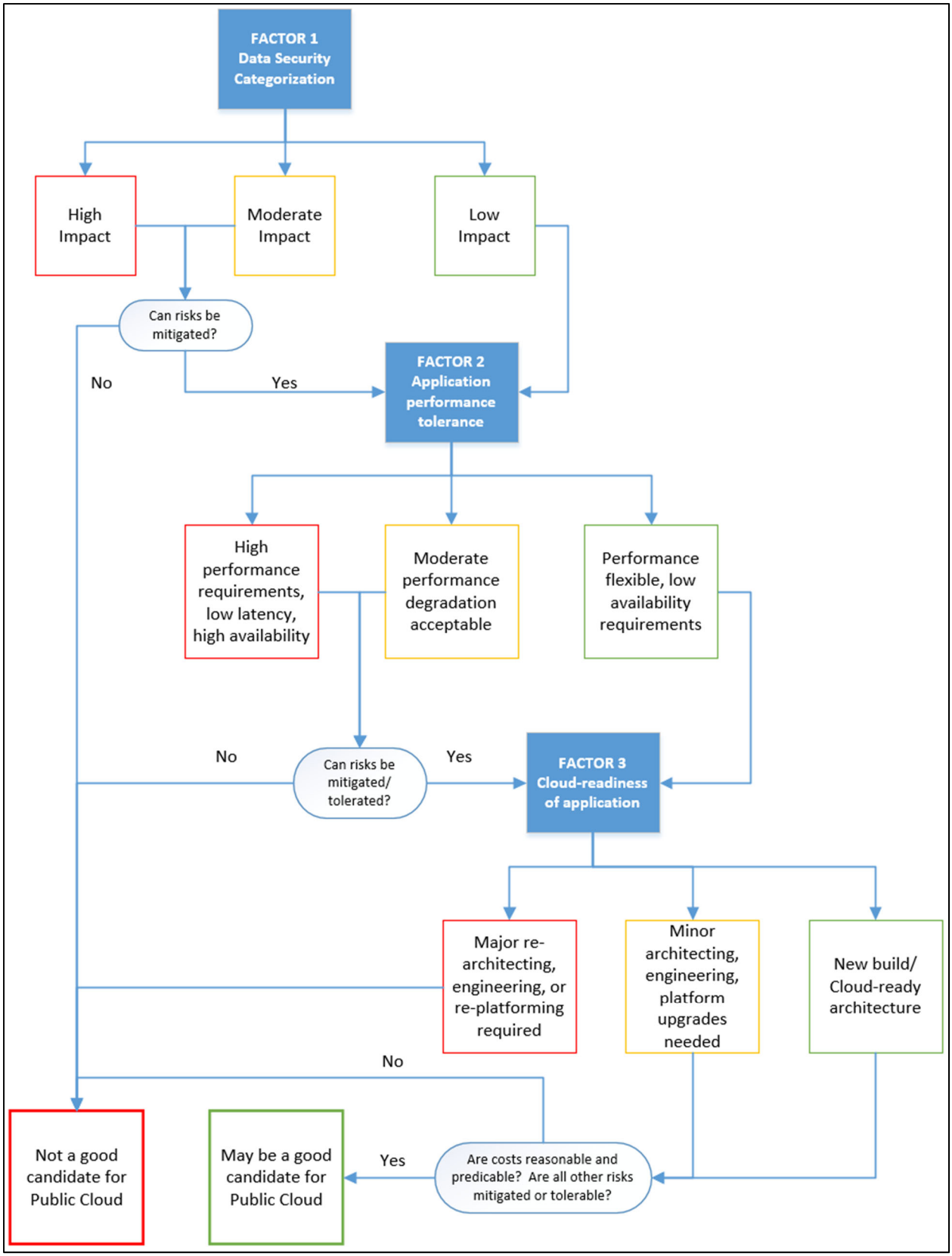

Figure 1 – Cloud Readiness Decision Tree

GUIDELINES

NJOIT will support public cloud computing with two distinct Enterprise Public Cloud (EPC) services: *Enterprise Public Cloud – Managed Hosting*, where NJOIT will provision public cloud computing resources for Agencies upon request, and *Enterprise Public Cloud – Self-Hosted*, where Agencies can self-provision public cloud computing resources within NJOIT's enterprise tenancy.

Existing Executive Branch public cloud subscriptions will transition to NJOIT's enterprise subscription as soon as possible, before the issuance of another initial commitment contract.

NJOIT and Agency Roles

NJOIT is responsible for shared services supporting both EPC services. Shared services include procurement and contract management tasks for the enterprise environment, private connectivity to the public clouds, enterprise-wide security and identity services, and internet ingress and egress access points connecting the public cloud to the internet.

Agencies are the users or consumers of the public cloud computing resources. Agencies are responsible for all costs associated with use of public cloud computing resources, whether provisioned in NJOIT's enterprise tenancy or otherwise. Agencies are also responsible for protection of the confidentiality, integrity, and availability for all their data and systems within the public cloud computing environment.

Agencies are responsible for understanding and identifying risks and costs involved with leveraging cloud computing services. Agencies can seek assistance from NJOIT and OHSP to assess and mitigate risks.

Agencies must review the NJOIT EPC Security Foundations and Responsibilities Overview document which provides details on the public cloud "Shared Responsibility" operating model that is essential for successful, secure consumption of public cloud resources.

Agencies that use the EPC–Self-Hosted service are solely responsible for the design and architecture of solutions deployed in the public cloud environments. However, NJOIT may deny requests to utilize shared services like internet ingress/egress gateways and direct circuits if the solution represents an unacceptable risk to the enterprise shared services or on-premises resources. Agencies should ensure full compliance with the SISM and all applicable laws, regulations, and adhere to cloud architecture best practices.

- **Access to the public cloud** is facilitated through either a virtual private network (VPN) connections or a direct private circuit, e.g. DirectConnect/ExpressRoute, and protected by next generation virtual firewalls. NJOIT is responsible for providing Agencies access to

these shared resources, which will be provisioned only upon written request from Agencies, which specifies the exact source and destination IPs. Access should be as limited as reasonably possible to meet business requirements.

- **Access from public cloud to the internet** is facilitated through virtual internet gateways existing within the public cloud. Because open internet access presents a potential risk to the entire public cloud entitlement and to on-premises resources via the direct connectivity with the public cloud, all internet access must be provisioned by NJOIT. Requests for internet access must be submitted in writing to NJOIT,[2] and non-standard requests may require conversations with the Office of Homeland Security (OHSP) and NJOIT's Internal Security Unit (ISU). In order to control risks presented by internet access, NJOIT and OHSP may request additional security controls or infrastructure architecture changes before internet access is approved and provisioned. Web application firewall (WAF) protection will also be required. NJOIT will administer distributed denial of service (DDoS) protection across the enterprise public cloud environments.

- **Intra-cloud communications**, meaning communications within virtual private clouds (VPCs) or subnets in a single public cloud service provider, are largely the responsibility of the Agency. However, communications between VPCs will require NJOIT provisioning as these communications are facilitated by shared resources.

PROCEDURE

Provisioning of Accounts/Subscriptions – <u>EPC-Self Hosted Service</u>
NJOIT is the enterprise account holder for EPC computing resources, which is available for NJOIT and State Agency use.

1. Provisioning of an EPC-Self Hosted account is done by service request to NJOIT. Accounts/subscriptions will not be provisioned until (1) a fiscal authorization is received from the respective using Agency, (2) Agency CIO approval is received, (3) a Privilege Escalation Form is submitted, identifying the Agency personnel with administrative privileges to the accounts and (4) an initial orientation meeting is held with the Agency, NJOIT and OHSP.[3]
    a. Fiscal Authorization
        i. Prior to the provisioning of an Agency's accounts/subscriptions, the Agency's fiscal team (CFO, etc.) must authorize the accrual of public cloud consumption charges, which will be charged back to the Agency via existing NJOIT cost allocation recovery (CAR) methodologies.
        ii. For NJOIT to adequately manage the availability of resources, the fiscal authorization must include the spend limit or budget that is approved by

[2] Note, workflows may vary as they are implemented into NJOIT's request provisioning system.

[3] Note, workflows may vary as they are implemented into NJOIT's request provisioning system.

the Agency. NJOIT will use this data to ensure that adequate entitlement exists across the enterprise accounts as well as to track Executive Branch cloud commitments.

iii. If applicable, an Agency must secure additional fiscal authorization to exceed an established spending cap. If an Agency exceeds its fiscal authorization, the account/subscription and all resources may be suspended to avoid accrual of consumption charges. *Exceeding fiscal authorization may result in sudden shut down or unavailability of an Agency's resources.*

b. CIO Approval
   i. Prior to the provisioning of an Agency's accounts/subscriptions, the Agency's CIO or equivalent must authorize the use of public cloud resources.

c. Privilege Escalation Form
   i. The provisioning and management of public cloud resources requires individuals with administrative rights to the account/subscription. NJOIT will provision administrative rights only to individuals documented and approved on a Privilege Escalation Form. Agencies are solely responsible for adding, managing, and deleting individuals with administrative access.

d. Orientation Meeting
   i. Prior to or in parallel with the provisioning of accounts/subscriptions, the Agency, NJOIT and OHSP will conduct an orientation meeting to discuss the enterprise public cloud offering, the shared services components, and the shared responsibility model for operations and security in the public cloud environments.
   ii. The orientation meeting will also discuss the Agency's anticipated use cases and the Agency's responsibilities regarding the Enterprise Public Cloud Portfolio logging.

2. Procurement/Billing
   a. NJOIT will provide Agencies with the credentials necessary to manage third-party cloud resources and to monitor the Agency's spend and consumption if such functionality is not available natively within the public cloud provider's portal.
   b. Billing for public cloud resources consumed will be submitted to the respective Agency via regular CAR billing; however, agencies may verify detailed consumption data within the public cloud portal. Resources consumed will be charged back according to the Agency and organization codes attributed to the account/subscription at initial provisioning. Agencies will also be billed for a percentage of costs of shared enterprise components including firewalls, connectivity port fees, and enterprise-wide security services.

Provisioning of Resources – EPC-Managed Hosting Service
Agencies interested in the EPC-Managed Hosting service should follow NJOIT's standard work/project intake processes on a project-by-project basis.

Change Management/CMDB Responsibilities
As NJOIT's third-party cloud environment is hosted and administered by NJOIT, IT Technical Staff must comply with NJOIT Circular 01-2014, NJOIT Internal Configuration Management and Change Control Policy, with regard to enterprise-wide and shared services resources.

NJOIT's Enterprise Public Cloud Portfolio
All staff engaged in development within NJOIT's Enterprise Public Cloud environment, including both the EPC-Self Hosted and EPC-Managed Hosting service offerings, are required to log their public cloud projects in NJOIT's Enterprise Public Cloud Portfolio and to tag cloud resources with the unique Portfolio ID Number. The Portfolio provides NJOIT and OHSP a single at-a-glance view of all projects and systems being developed and hosted in the public cloud.

a. Access. For role-based access to the EPC Portfolio website, please email epc-mh-prod@tech.nj.gov.
b. Portfolio ID Number. Entry of a project in the Portfolio automatically assigns a unique Portfolio ID Number for tagging of assets in the public cloud. All staff must tag assets in the public cloud with the Portfolio ID Number for correlation with logged projects. NJOIT and OHSP will conduct verification and audits of tags to ensure and encourage compliance.
c. Updates. All staff must update and edit Portfolio entries from time to time, as needed.
d. Prerequisite Entry. Before NJOIT will provision access to the public cloud, access to the internet, or intra-cloud communications described above, the system or project at issue must have an up-to-date Cloud Portfolio entry(ies). Staff are encouraged to include the Cloud Portfolio ID Number in all provisioning requests submitted to NJOIT or OHSP.

SCOPE

All Executive Branch departments and State agencies (Agencies) are directed to cooperate fully with the NJOIT and the CTO to implement the provisions of the Policy, and to ensure effective use of information technology within the Executive Branch of State Government.

AUTHORITY

New Jersey Statutes Annotated (N.J.S.A.), Sections C.52:18A-224 through C.52:18A-234, known as *"The Office of Information Technology Reorganization Act."*

NJOIT reserves the right to change or amend this Policy to comply with changes in Agency procedures. Any changes or amendments will be announced and made available on NJOIT's Intranet under Policies. Changes in this Policy will be effective upon such publication or distribution.

TERMS AND DEFINITIONS

The definitions for terms in this Policy can be found in the NJOIT Policy Glossary located at:
http://highpoint.state.nj.us/intranets/oit/policies/glossary.html
http://www.nj.gov/it/business/index.shtml#glossary

Additional definitions can be found in the Statewide Information Security Manual (SISM). For the most recent publication, refer to: https://www.nj.gov/it/services/policies.shtml.

Cloud Computing - A model for enabling on-demand network access to a shared pool of configurable IT capabilities/resources, e.g., networks, servers, storage, applications, and services, that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them.

This cloud model is composed of the following three clusters.

Five (5) essential characteristics: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service.

Four (4) models for enterprise access: private cloud, community cloud, public cloud, and hybrid cloud.

Three (3) service delivery models: cloud software as a service (SaaS), cloud platform as a service (PaaS), and cloud infrastructure as a service (IaaS).

Cloud Service Provider - is an entity that offers cloud-based platform, infrastructure, application, or storage services. Cloud service providers include internal entities, such as NJOIT, and external entities, such as Amazon, Microsoft, Salesforce, Google, and others.

SIGNATURES

SIGNATURE ON FILE **02/20/2020**

CHRISTOPHER J. REIN **DATE**

Chief Technology Officer-NJ Office of Information Technology

DOCUMENT HISTORY

Printed copies of this document are uncontrolled; please refer to the NJOIT website for the current version in effect. Please visit our website at: *www.tech.nj.gov*

Version	Published Date	CTO	Sections Modified	Description of Modifications
1.0	02/20/2020	C. REIN	NEW	Original Published Date