Division of Enterprise Technology

Cloud Advantages/Disadvantages – REFERENCE DOCUMENT

Table of Contents

Purpose 1

Background 1

Guidance 2

Benefits and Risks 2

Key Considerations 4

Additional considerations 6

References 8

Document History/Owner 9

Purpose

This reference document explains the components of the advantage/disadvantage assessment included in the Agency Cloud Solution Information Form.

Background

Cloud computing represents a major trend in the IT industry. The State of Wisconsin has been selectively utilizing Cloud solutions at an increasing rate. Cloud solutions are being considered on a case-by-case basis, following a cloud appropriate model.

Current drivers of cloud adoption for the State of Wisconsin generally include the following:

- Vendors moving software to a subscription model offering Software as a Service (SaaS) in the cloud (i.e., Office Productivity from Microsoft 365)
- Unmet needs addressed by implementing new SaaS applications (i.e., Electronic Medical Record from Cerner Millennium)
- New capabilities provided (or currently under review) as Platform as a Service (PaaS) to support application modernization efforts and other requirements (i.e., Credential Store from Amazon Web Services, AI from Google, etc.)
- Security hardening has been or will be provided by cloud solutions (Vulnerability Scanning from CrowdStrike, External User Account management and Authentication from Okta, etc.)
- Applications have been refactored when they have outgrown their current platform due to increasing requirements or volume (i.e., SharePoint apps rewritten using Low Code platforms in the cloud)

To further define cloud trends, the Federal government recently updated their cloud strategy from “Cloud First” to “Cloud Smart”. The following experts from the Federal Cloud Computing Strategy highlight this approach:

- The term “cloud” is most accurately applied to those solutions that exhibit five essential characteristics of cloud computing, as defined by NIST: on-demand service, broad network access, resource pooling, rapid elasticity, and measured service (see definitions section).
- These characteristics and the solutions that exhibit them are provider-agnostic – meaning anyone can develop and deploy a cloud solution, whether an outside vendor or a Federal agency.
- Industries that are leading in technology innovation have also demonstrated that hybrid and multi-cloud environments can be effective and efficient for managing workloads.
- Agencies should assess their requirements and seek the environments and solutions, cloud or otherwise, that best enable them to achieve their mission goals while being good stewards of taxpayer resources.

Guidance

Benefits and Risks

The cloud computing business model to deliver technology as a service (software-SaaS, platform-PaaS, and infrastructure-IaaS) presents a compelling opportunity to agency leadership to address critical IT issues including increased cost efficiency, provisioning speed, scalability, and life cycle management. However, cloud computing introduces risk into agency’s technical and business environment that must be weighed against those benefits. Risks include data security, loss of control, interoperability, and hidden costs. Given the potential benefits and risks of cloud computing, agencies will need to analyze and identify opportunities to take advantage of cloud computing in certain situations when risk can be minimized or mitigated with confidence.

Benefits

Benefit of Reduced cost

A potential benefit of cloud computing is IT cost savings. Under the cloud computing model, the costs of acquiring, maintaining, and refreshing software, tools, development platforms, hardware, storage, etc. are shifted to the cloud service providers (CSPs). CSPs can serve a high number of customers and they are able to offer lower individual pay-per-use rates by leveraging economies of scale, commoditizing infrastructure, and automating data center processes.

Benefit of Provisioning Speed

Another typical pain point in IT is provisioning speed. Providing new applications, setting up technical environments, developing new software, etc. may take a long time and it is often not aligned with changing business needs and customer expectations. A key characteristic of cloud computing is the automated provisioning of computing resources and it has the potential to increase provisioning speed. For instance, think of a potential scenario where the need for a data and financial analysis tool is presented. The required functionality is already provided in the form of Software as a Service (SaaS) by an authorized CSP. Authorized users in the business and financial teams may get almost immediate access to the SaaS capability on a pay-per-use model. There would not be a need to procure a server, software, connect it to the network, and provide access, before users can use the functionality.

Benefit of Scalability

To take advantage of economies of scale, CSP data centers have massive amounts of computing resources (memory, CPU, storage, etc.) available automatically to cloud service consumers. Individual program needs for computing resources may vary for several reasons. An unexpected event, new policies or regulations may trigger increased demand for computing resources that was not forecasted in advance. Cloud computing offers the potential benefit to both scale up and down computing resources as needed.

Benefit of Agility

The cloud service provides include several capabilities to support agile approaches, including servers, containers, and components on demand. These capablitiies and others support the notion of continuous integration, deployment, and delivery (aka CI/CD).

Benefit of Lifecycle Management

In a cloud computing model, the CSP owns the responsibility to ensure software and hardware remains current. The CSP will plan, test, and deploy software and hardware upgrades as necessary to keep technology current.

Benefit of Security

Cloud computing vendors frequently allocate significant resources (both people and money) to securing their solutions as breaches or other security issues can cause significant or complete loss of business. The use of independent audits, SOC reports, FedRAMP compliance, and other similar activities drive transparency and clarity of what the vendor is doing to protect the system, data, facilities, etc. associated with the solution they are providing. Since cloud providers support hundreds or thousands of customers, they are able to make more significant investments in security that all can benefit from.

Additional Benefits include

- Connectivity from anywhere
- Pay-as-you-go model
- Innovative technologies more accessible such as AI, Machine Learning, IoT, microservices, …
- Data sharing
- Robust DR/Availability/Resiliency

Risks

Risk of Data Breaches

While the benefits of cloud computing appear attractive, several risks are introduced under the model. The maturity of cloud models is increasing. However, there is also increasing volume and sophistication of cyber intrusions on the Internet that bring significant risks to the Department's protected data.   The Department could risk law suites, government fines and loss of public confidence if its sensitive data were released to, or acquired by, unauthorized personnel.   As such, moving agency information into commercially provided clouds that operate outside of agency security protections and operational control can increase these risks.

Risk of Limited Interoperability

Lack of interoperability and Integration is a critical risk for Enterprises moving to the Cloud. With SaaS, there is limited ability to access the data directly – all access is controlled by the SaaS application. Access to the data may be provided through SOA, or a lighter weight and increasingly more common RESTful API. Still, even with published APIs, there is a great deal of complexity in integrating multiple SaaS and legacy on premise systems. Interoperability between SaaS systems, other Cloud applications, and legacy applications should be a major concern of the agency.

Risk of Performance Degradation, Outages

One characteristic of cloud computing is delivery of services over a network, typically a Wide Area Network (WAN), such as the Internet. While this characteristic provides benefits, it also presents a critical challenge, especially for systems used by many offices across the state within or across agencies. Degraded network performance and/or substandard application performance at the Cloud Service Provider's location can have a negative impact on agency operations. At extreme levels, the solution may experience outages/downtime, denial of service (technical or financial), resource exhaustion (under or over provisioning), and aggregation risk (too many customers on too little infrastructure).

Risk of Hidden Costs, Vendor Lock-in

Assess the overall cost of delivering a Cloud Service Provider's service capability. Pricing is increasingly complex as the vendors and product variations grow. But even if the agency gets past that pricing complexity to pick the right vendor at the right price, the agency may face the problem of getting clear visibility into how the charges are run up. Moreover, ramp-up costs can add up, especially when seemingly minor decisions upfront turn into unnecessary ongoing expenses. Cloud computing can lead to a sense of infinite computing resource availability which, in turn, can eventually foster escalating costs over time. This involves the risk of cost increases either from increased usage and/or increased fees. In addition, vendors may increase rate over time which is a real issue as it becomes more difficult to move the solution to other providers, creating a vendor lock-in situation.

Additional Risks

- Defensive IT security depth may be lacking, potentially exposing information with one mistake
- Cloud provider acquisition, supply chain failure
- Exit strategy, data hostage risk, incomplete data deletion in cloud
- Subpoena and e-discovery support
- Insufficient indemnification of liability, privacy, and data security concerns
- Cloud provider may share regulated data with other cloud providers, potentially leaking sensitive data to the public

Key Considerations

Before moving forward with a cloud solution, it is important to consider several factors. The following is not intended to be a comprehensive list, although, provides guidance to agencies when considering cloud-based solutions. This list is an excerpt from a Gartner research paper titled “Developing a Practical Hybrid Workload Placement Strategy” plus a few others.

Compliance

Are there regulatory or compliance issues with this service, and if so, are there providers certified at the level that would satisfy my audit and compliance requirements?

Data protection

Are there data protection, access, backup or compliance issues with the inputs or outputs of this application, and can providers satisfy these issues?

Security

How critical are the security and access control requirements for this application, and can they be implemented and managed to satisfy internal corporate security requirements?

Latency

When operational, how much impact will latency have on application acceptance and customer usage patterns? Will reduced latency (or variable performance) impact customer satisfaction, or possibly corporate reputation?

Recovery time

What recovery time and/or recovery point objectives are needed for this application, and can they be satisfied with an external provider or only via internal processes?

Impact of outage, Reputation

What impact will service outages have on corporate reputation and/or client satisfaction, and can this be mitigated by outside providers?

Service continuity

How important is service continuity to our success? Is the perception of 100% availability required, and if so, can providers or the providers' solutions be structured to deliver this at a reasonable cost?

Performance

What is the impact on poor or variable application performance? Are tools available for remote monitoring and problem resolution?

Data location

Are there any issues with guaranteed data location? For localized (in-region) applications, this may not be an issue, but for global deployments, it may be critical.

Availability

What are the availability goals, and what will be the impact on business operations if they cannot be met?

Additional considerations

Transfer risk, ensure proper controls are implemented

[Write more about defensive depth, terms covering data protection and security practices. Include penetration testing, inspections, or certifications.]

Vendor management

Vendor management is a critical aspect of cloud computing beginning with procurement, through contract management, and especially termination. Vendor Management involves understanding the governance and management of the solution being provided including the roles and responsibilities of the customer vs. the vendor and who is accountable for what. Vendor management should focus on win-win scenarios where both the vendor and the state benefit from the relationship which is built on a foundation of partnership. A vendor management plan for both the implementation of the system and ongoing operations of it should be developed.

Contract management

Utilization of existing contracts (i.e., NASPO Cloud Contract) provides the ability to cover many of the risks and considerations listed within this document. It will be important to understand the scope of existing contracts and add additional terms to address expectations (i.e., service levels) and specific risks related to the solution being procured. For new contracts, it will be important to start with model contract cloud terms to cover common expectations and risks. Establishing a well-documented support model and escalation process will help address risks. Terminating a cloud contract can be difficult. Contract terms need to be identified up front to describe how data will be returned (among other things) to the agency at contract end. Protections need to be established to ensure the cloud provider does not degrade performance, increase rates, or exhibit other bad behavior once notified about contract termination.

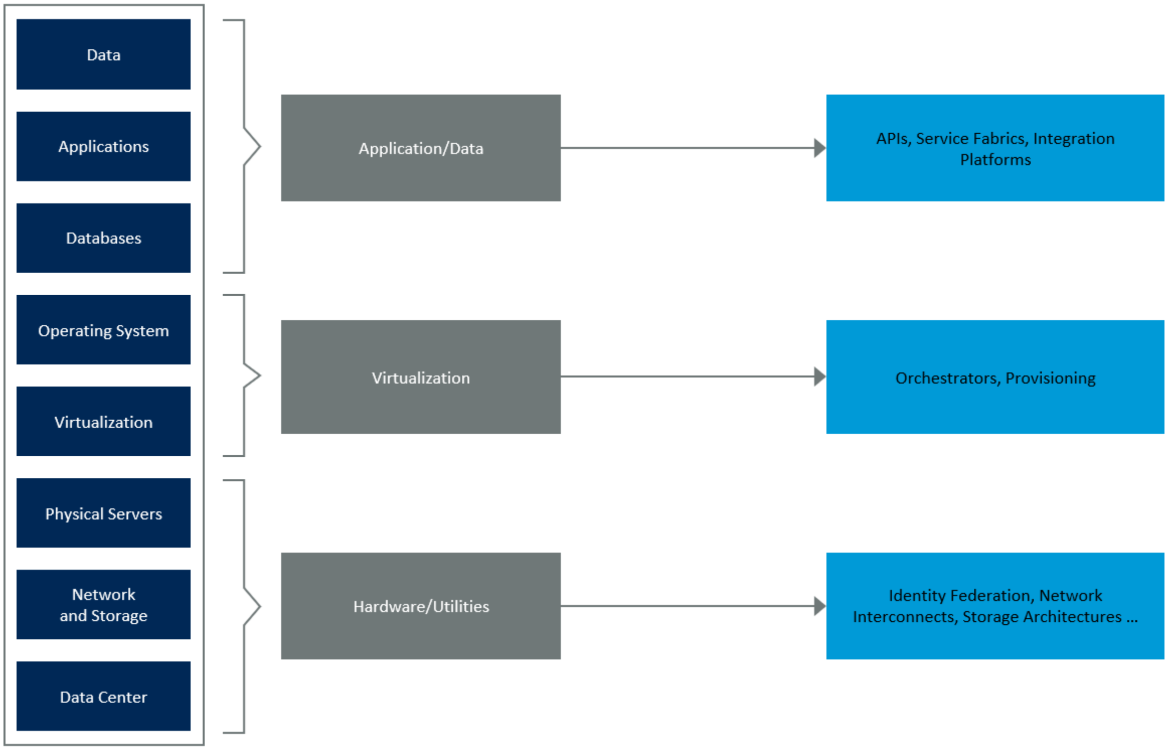
Location of data and staff

It is important to note that many compliance standards (i.e., CJIS) include a requirement to house all data in the United States. In addition, Act 136 prohibits state contractual services to be provided outside of the United States, although, exceptions may apply (i.e., services not available, federal funding, etc.).

Hybrid Cloud

Does the solution require connection between the DET on premise data center and the cloud provider data center? If so, how will this be accomplished? Gartner has provided a framework to approach this question. Options are divided into three distinct categories including application/data, virtualization, and hardware/utilities.

Levels Where Integration Occurs



Source: Gartner
ID: 407153

Multi-cloud

Will the solution utilize more than one cloud provider? Management of multiple cloud providers may introduce additional management challenges and risks. For example, contracts may not include the same service levels, termination dates, or escalation path. The support model for these types of solutions will need to address this added level of complexity. In addition, it will be important to understand the type and depth of integration necessary to implement and operate the solution.

Roles and responsibilities

Consider how the cloud solution will be procured, implemented, and supported. Include roles from business areas, procurement, legal, agency and enterprise IT. Also identify the cloud vendor roles and responsibilities. Refer to DET Service Offering Definition and Role and Responsibilities as needed.

References

Gartner research “Developing a Practical Hybrid Workload Placement Strategy”, Refreshed: 8 October 2018 | Published: 30 June 2017 ID: G00326132.

Additional Gartner research “Using Hybrid Architectures for Cloud Computing”, “Gartner Predicts By 2023 Over Half of Government IT Workers Will Occupy Roles That Don’t Exist Today.”, and “Most New Government Technology Solutions Will Be Delivered and Supported Using a XaaS Model by 2023.”

Federal Gov CIO: From Cloud First to Cloud Smart In the Report to the President on Federal IT Modernization, released publicly in 2017 in accordance with Executive Order 13800.

Federal Cloud Computing Strategy

NIST Special Publication 800-145 - The NIST Definition of Cloud Computing provides definitions for service models (SaaS, PaaS, etc.), deployment models (Public, Hybrid, etc.) and essential characteristics

ManageEngine: Cloud Isn’t Always the Answer: Issues to Consider Before Migrating to the Cloud by Kamala Kannan Subramani

Accenture: Hybrid cloud: Enabling the rotation to the New

Deloitte: Tech Trends 2019, Beyond the digital frontier: Deloitte Insights 10th Anniversary Edition

Act 136 foreign purchases

Cloud Security Alliance: Cloud Controls Matrix Version 3.0.1

Google Cloud Compliance - Regulations & Certifications

AWS Data Classification Secure Cloud Adoption March 2020 and Compliance standards united states

Microsoft Azure Compliance in the trusted cloud

StateRAMP to Offer State, Local Government - Secure Vendor Pool BY: Skip Descant GovTech

DevOps Cloud CoE Report – State of WI Draft: Ahead

DOC Enterprise Cloud Strategy V3.2

Cross agency input from DOA, DOT, DHS, ETF, and others

Document History/Owner

Version	Approval/Revision/ Review Date	Approver/Author-Title	Description

Authorized and Approved by:

Print/Type Title Signature Date