Innovative. Open. Agile.

TechFlow, Inc. Response to
Request for Quotation (RFQ)
4QTFHS150004
Agile Delivery Services (ADS I)

Cloud Solution Checklist

July 7th, 2015

TECHFLOW

TABLE OF CONTENTS

LIST OF FIGURES

1.0 Overview

This document has been developed as a checklist to assist with the migration to a cloud based solution. With this

2.0 Approach

When developing your cloud strategy you first need to determine what you will be building in the cloud is it a new application or is it the migration of a legacy application. Other points to consider are:

- Application size to include functionality and data
- Application complexity
- COI
- Application and Data security requirements

Once the information has been developed the attention should now focus on what is available in the markets space whether its commercial or government. Below are the primary options available:

- Software-as-a-service(SaaS): This option involves the vendor running your software application for you, so that your business doesn't have to buy a software license from Oracle or Microsoft or other providers.
- Platform-as-a-service (PaaS): The vendor provides and manages for you the operating system and the database and everything else you need to run certain platforms.
- Infrastructure-as-a-service (IaaS): This used to be known as "utility computing," wherein the vendor supplies the network and servers and your business uses that infrastructure and pays for what it uses in terms of capacity and storage.

There are other cloud services but these have emerged as the foundational offerings. When making a decision its important to consider what level of i.t. support you will need. If you do not have seasoned developers and/or administrators you may want to consider the software as a service platform which requires the lease amount of internal i.t. support. If you have an application development staff either the platform as a service or infrastructure as a service could be leveraged because you will have the ability build and modify your own applications. Furthermore PaaS and IaaS give you the ability to determine your usage based on needs and you can quickly throttle up or down.

3.0 Cloud Considerations

Once you have identified the type of service you need the next step is to determine which provider you will choose. There are many vendors in all aspects of cloud offerings so we recommend to document and prioritize your solution criteria prior to any vendor discussion. Most vendors will give you a trial license and we strongly recommended that you take advantage of these trial offering to better understand the usability. Figure 1 is a high level process used to illustrate the process:

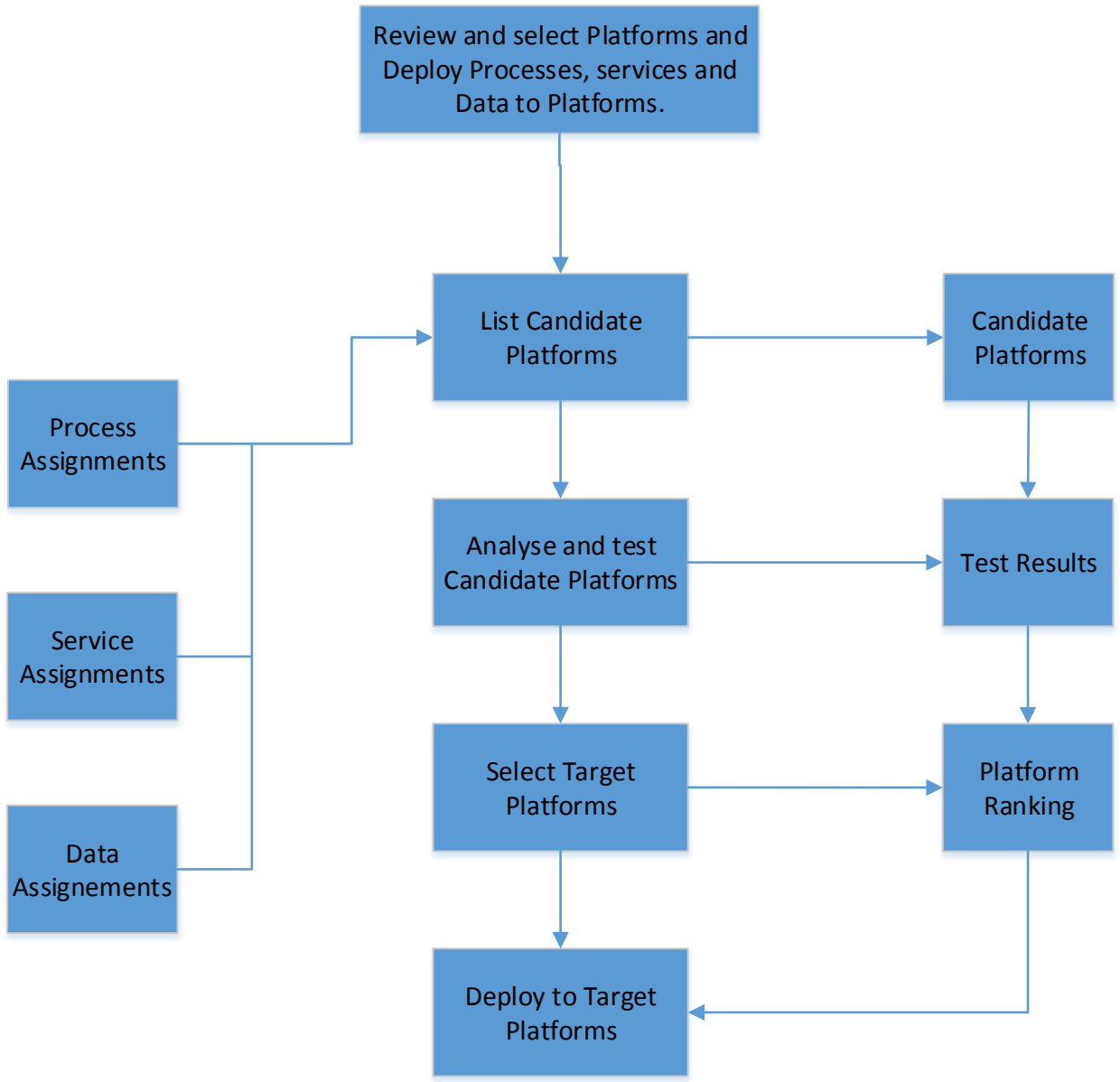

Figure 1. Cloud Evaluation Process

4.0 Cloud Solution Checklist

Now that we have discussed strategy at a high level and the preliminary work has been done, we will get into a detailed checklist to ensure completeness of your solution:

Cloud Solution Checklist			
Area	Topic	Specific Concerns	Answer
Security and privacy	Data protection	Data segregation	
		How do you separate my data from other customers' data?	
		Data-at-rest protection	
		Where do you store my data?	
		How strong is your encryption and data integrity?	
		What kind of authentication and access control procedures are in place?	
		Documentation for auditors	
		Data-in-motion protection	
		How do you get data from me to you?	
		How do you transfer data from one place to another?	
		What are your data leak prevention capabilities? (if applicable)	
		Can any third party (your service providers) access my data, and if so, how?	
		Can you ensure that all my data is erased at the end of service?	
	Vulnerability management	Can you show evidence of your vulnerability management program?	
		How often do you scan for vulnerabilities on your network and applications?	
		Can I conduct an external vulnerability assessment on your network, and if so, how?	
		What is your vulnerability remediation process?	
	Identity management	Can you integrate directly with my directories, and if so, how?	
		Review the architecture of integration.	
		Ensure it doesn't create a security risk for my own infrastructure.	
		If you keep your own user accounts:	
		How do you secure user IDs and access credentials?	

Cloud Solution Checklist			
Area	Topic	Specific Concerns	Answer
		How do you handle user churns (e.g., provision and deprovision accounts)?	
		Can you support SSO, and if so, which standards?	
		Can you support federation, and if so, which standards?	
	Availability	How many nines do you guarantee in the SLA?	
		What availability measures do you employ to guard against threats and errors?	
		Do you use multiple ISPs?	
		Do you have DDoS protection, and if so, how?	
		Can you provide availability historical data?	
		What is your downtime plan (e.g., service upgrade, patch, etc.)?	
		What is your peak load, and do you have enough capacity for such a load?	
	Application security	Do you follow OWASP guidelines for application development?	
		Do you have a rigorous testing and acceptance procedure for outsourced and packaged application code?	
		What about third-party apps (components) that you use in your services?	
		What application security measures (if any) do you use in your production environment (e.g., application-level firewall, database auditing)?	
	Incident response	What is your procedure for handling a data breach?	
		Can notification occur within a specified time period?	
		In what format do notifications go out, and what info do they contain?	
		Ensure that the vendor's incident response procedures do not violate our own incident response requirements.	
	Privacy	Ensure that critical data (e.g., payment card number) is properly masked and that only authorized individuals have access to the entirety of the data.	

Cloud Solution Checklist			
Area	Topic	Specific Concerns	Answer
		Show me how you protect digital identities and credentials and use them in cloud applications.	
		What data do you collect about me (logs, etc.)? How is it stored? How is the data used? How long will it be stored?	
		Under what conditions might third parties, including government agencies, have access to my data?	
		Can you guarantee that third-party access to shared logs and resources won't reveal critical information about my organization?	
	Business continuity and disaster recovery	Do you have any DR and BC planning documents, and if so, can we review them?	
		Ensure that the procedures are at least as robust as our own.	
		Can we do a BC audit?	
		Where are your recovery data centers located?	
Compliance		What service-level guarantee can you offer under DR conditions?	
	Logs and audit trails	Can you accommodate timely forensic investigation (e.g., eDiscovery)?	
		Can we agree on provisions in the SLA for investigation?	
		What would we have access to? How?	
		How long do you keep logs and audit trails? Can you keep them as long as we desire?	
		Can we have dedicated storage of logs and audit trails, and if so, how?	
		Show evidence of tamper-proofing for logs and audit trails	
	Specific compliance requirements	Are your data centers under local compliance requirements? If so, which ones?	
		Do the local compliance requirements violate our own?	
		Are you SAS-70 compliant (if applicable)?	
		Are you ISO-27001 compliant (if desired)?	
		Can you prove that you are compliant for:	
		California A.B. 211?	

Cloud Solution Checklist			
Area	Topic	Specific Concerns	Answer
		PCI ?	
		HIPAA?	
		Basel II?	
	Business continuity and disaster recovery	Do you have any DR and BC planning documents, and if so, can we review them?	
		Ensure that the procedures are at least as robust as our own.	
		Can we do a BC audit?	
		Where are your recovery data centers located?	
Compliance	Liability	What recourse actions (e.g., financial compensation, early exit of contracts, etc.) can we agree on in the event of a security incident or failure to meet SLA?	
		Under what conditions . . . ?	
	Intellectual property	Can we stipulate in the SLA that all my data (or applications), including all replicated and redundant copies, are owned by me? Ensure that your service agreement does not lead you to relinquish any IP rights.	
		Scrutinize the language in the terms-of-service that govern the ownership of and rights to information that you place in the cloud.	
Other legal and contractual issues	End-of-service support	Specify what the cloud vendor will deliver at the end-of-service period.	
		Will data be packaged and delivered back to me? If so, in what format?	
		How soon will I have all my data back?	
		Will any remaining copies of data be erased completely from your network? If so, how soon will it happen?	
		Specify any fees that may incur at the end of the service.	
	Liability	What recourse actions (e.g., financial compensation, early exit of contracts, etc.) can we agree on in the event of a security incident or failure to meet SLA?	
		Under what conditions . . . ?	

Cloud Solution Checklist			
Area	Topic	Specific Concerns	Answer
	Intellectual property	Can we stipulate in the SLA that all my data (or applications), including all replicated and redundant copies, are owned by me? Ensure that your service agreement does not lead you to relinquish any IP rights.	
		Scrutinize the language in the terms-of-service that govern the ownership of and rights to information that you place in the cloud.	
Other legal and contractual issues	End-of-service support	Specify what the cloud vendor will deliver at the end-of-service period.	