NEW WORLD TECH

TOP RISKS IN CLOUD MIGRATION

WHITE PAPER

CONTENTS

ABSTRACT

Cloud is an indispensable part of the IT world today, its flexibility and scalability are the features that have been long-awaited in the market. When it comes to a migration to a Cloud, a number of risks related to a customised target (Future Mode of Operation) have simply vanished. However, the risks related to the migration project itself and the source infrastructure (Current Mode of Operation) are still relevant.

Each Migration Project is about Transforming one IT environment into another. Twenty years ago both were highly customised, but over the years the target environment (FMO) has become more and more standardised, front-end and back-end platforms and processes etc. As a result each new outsourcing contract and transformation project started from a more standardised environment than the previous one.

The same applies today, the targeted cloud environment (FMO) will be, in large majority of cases, much more standardised than the starting (CMO) one. This means that like any time before we will be moving a less standard environment into the standardised one and that is not an easy task, it definitely creates some risks… and that is what this white paper is about.

INTRODUCTION

Migration to cloud is the logical continuation of the traditional IT outsourcing practices. The main business goals remain cost optimisation, improved performance and access to the cutting-edge IT technology, while getting more time to focus on the core business (for non-IT companies).

The evolution of the traditional outsourcing approach could be divided in multiple phases:

The first generation of outsourcing where the whole infrastructure was managed in-house. It basically means that, in the full-scope outsourcing deals, a Service Provider would take over the back-end server infrastructure, front-end user infrastructure, service management, service desk and a large number of employees.

Cost reduction was achieved through the consolidation of multiple data centres into fewer locations (typically twin data centre for each major region). Further costs were saved through the replacement of old (often mainframe) technology with the energy efficient computers, reduction of number of service desk languages, standardisation of end-user devices (including applications) in order to automatise their maintenance and streamlining of service management processes. Through this process it was necessary to transform/adjust the applications that were running on the old infrastructure.

In the second generation the clients who had already gone through the first generation outsourcing were looking for further automation and cost optimisation of their services. This was achieved through server virtualisation, thin-client introduction, proactive maintenance using data analytics and, more than in the first generation, application optimisation. In the second generation there was already partial introduction of bespoke private clouds, either from the client or Service Provider premises.

THE MAIN CHALLENGES

The main clients' challenges that were only partially resolved by the first two outsourcing generations were:

- **Inflexible billing model** – the contracts were by default based on a fixed price, with some adjustments based on the ARC (additional resource charge) and RRC (reduced resource charge) model. In this model there was a significant time lag before the change in the resource consumption would be reflected in the billing model.
- **Insufficient flexibility and scalability** – as the outsourced infrastructure was planned and allocated to a single client, Service Providers did not have an option to allocate unused resources to different clients on a per need basis. This meant that there was no dynamic increase or reduction of capacity.

MAIN MIGRATION RISK GENERATORS

The main migration risk generators in the traditional outsourcing models mentioned above are listed below. They presume that a Service Provider would execute migration/ transformation to cloud on behalf of the client and will sign off an overall outsourcing contract with it:

1. **Insufficient information on the CMO**, i.e. the existing client IT environment, which is a starting position for the migration.

2. **Misinterpretation of some client's requirements** leading to the FMO (final/future mode of IT service operation created through the Transformation/migration process) that does not meet clients expectations. It obviously creates deep client's dissatisfaction and also leads, in some cases, to significant financial loses on the client and/ or Service Provider side.

3. **Unclear Roles and Responsibilities (R&Rs)** during the transformation/migration process. Service Providers depend heavily on client knowledge and actions in some areas (for example, in-house developed applications that are in scope for the migration/transformation). Also, there might be unclear R&Rs between the Service Provider and current/ future third parties that are involved in the migration programme and/or the following ongoing service delivery.

4. **CMO service management tools/processes owned by the client are missing some critical parts**, for instance incomplete/inaccurate CMDB (configuration management DB), missing user information etc.

5. **CMO Service management tools/processes are not easily transferred/integrated** with the FMO Service management tooling due to the data / process incompatibility.

6. **Decentralised security management in the CMO environment**, for example, client separately manages security for servers, clients, apps, network etc. Migrating such an environment to the centralised FMO security domain managed by a Service Provider is a daunting task.

7. **The CMO IAM (Identity and Access Management) versus the FMO IAM solution**. The current state of Active Directory and its integration with service management, email tools etc. does not provide a good basis for a smooth transformation/migration to the FMO.

8. **The linkage between transformation/migration and projected cost reductions it is unclear.** Lack of clarity on how the completion of specific migration/ transformation activities leads to the cost reduction, especially in the situation where certain activities cannot be treated in isolation. For instance, virtualising number of physical servers does not create cost reduction if the physical servers cannot be decommissioned yet. The reason could be that some apps are still sitting on them and are yet to be migrated.

9. **Unclear strategy for apps migration/ Transformation,** i.e. which ones should be virtualised, migrated or kept unchanged on physical legacy servers. It is often related to insufficient apps documentation, especially when it comes to legacy, in-house developed software.

10. **The migration/Transformation Plan does not address how to deal with the client's** in-flight projects that will be running in parallel with migration and will sometimes create strong dependencies and priority clash.

CLOUD MIGRATION SPECIFIC RISKS

Introduction of cloud services could be considered as a cornerstone for the **third outsourcing generation**. It addresses to a great extent the main client challenges not resolved by the previous outsourcing strategies – inflexible billing and limited scalability/capacity flexibility.

However, the migration/transformation to cloud still encompasses all "traditional" risks listed above, plus some additional ones. Again, the presumption is that a Service Provider would execute migration/transformation to cloud on behalf of the client and will sign off an overall outsourcing contract with it:

11. **FMO Architecture is pretty much predefined,** i.e., each CSP (Cloud Service Provider) offers predominantly standardised services. This creates a challenge in the situation when the CMO environment is incompatible with the targeted FMO services. In the traditional outsourcing approach the client can ask for a bespoke FMO that would be compatible with its CMO situation, but that level of flexibility is unavailable with the cloud-based solution.

12. **Lack of clear migration/Transformation strategy,** some clients rush to move to cloud in order to improve their operational efficiency. This can result in a long and expensive migration/transformation and even, in some cases, unresolvable issues (for example, incompatibility with the selected cloud services).

13. **Security**, CSPs typically provides security at the infrastructure level, while the client is responsible for the internal security, for example, data protection, application protection etc. It might be a big challenge to get a full security control in the world of divided responsibility, especially for the client with strict security and privacy regulations.

14. **Cloud billing system can be very complex,** especially for Enterprise solutions. The clients may not understand how different service offerings fit together, which may in turn lead to unnecessary, redundant subscriptions and cost overrun.

15. **Integration of Service Providers**, if multiple Service Providers work on the migration/transformation to cloud (for different services) there is a risk that the work will not be coordinated among them and the selected CSP.

RISK RESPONSE

For the above outlined risks the following mitigation actions could be taken when performing migration/Transformation to cloud:

a) Lack of the information on the CMO can be addressed through extensive Due Diligence (DD) process performed by the client before making any migration/transformation plans. This activity should be done by deploying internal resources, discovery tools, external experts, future Service Provider and whoever is needed to understand its environment end-to-end.

b) The understanding of client's requirements should be validated by a Service Provider during the negotiation or, at latest, during the creation of a detailed Execution Plan. Client requirements should be checked out not only with the client, but also with the selected CSP and potential third parties in order to understand if the requirements are compatible with the CSP services. In the cases where the client's requirements are missing in some areas, Service Provider should make assumptions based on best practices and validate them with the client and other involved parties.

c) Roles and Responsibilities (RASCI table) should be one of the key aspects of each outsourcing contract. A small omission in R&R can cost a lot of money and bring the programme to a standstill.

d) As part of the DD process described in a) above, maturity assessment of the current service management environment should be done. This would include the quality of CMBD data, the quality of Asset management data, User information (in Active Directory and elsewhere), Procurement records and alignment between all these data sets. Further, the consistency and integration of Event management processes (Incident, Problem, Change management) should be validated.

e) Once the DD activities outlined in d) above have been completed, the team should analyse Service-Management-in-cloud offerings from different CSPs. Typically this analysis would be done together with the Service Provider that would be executing the migration/transformation programme. During this exercise one or more CSPs should be selected as well as the scope of the service management programme. One of the key questions to be answered is how to integrate service management process for the infrastructure parts inside and outside the cloud (if part of the infrastructure remains outside the cloud).

f) Security should be one of the key elements, together with Apps and service management compatibility, in deciding what cloud migration/transformation strategy to choose, i.e., if it would be public, private or hybrid cloud. In order to get there the client should first connect the dots (alone, or with the help of a future Service Provider) on the CMO security setup and understand clearly existing interdependencies before moving to the service mapping with potential cloud security offerings.

g) IAM policies and the alignment of user data in the current client environment (CMO) is the prerequisite for the successful migration/transformation to cloud. Therefore, as part of internal DD process (with or without the help of future Service Provider) the integrity of data and policies need to be validated and strengthened wherever needed.

h) The Migration/Transformation Plan needs to identify chunks of migration work that, when completed, can move into the FMO state and, independently of the remaining migration activities, start utilising lower operational cost based on the cloud billing method. These milestones need to be clearly outlined in the project plan and they, together with the associated cost savings, represent the basis of the Migration/Transformation Business Plan (and overall Outsourcing Business Plan). This projection should be created by the party that performs migration/transformation (Service Provider or the client itself).

i) As indicated earlier apps migration/transformation is, together with Security and Service Management, a key driver in the process of devising migration/transformation strategy. Compatibility of application with the FMO cloud environment, criticality of application and data associated with it, special compliance requirements linked to some applications etc. are the elements to be taken into account when contemplating the scope of the application migration in relation to the choice of the CSP. This analysis, again, can be done alone by the client or in cooperation with the Service Provider.

j) The client needs to align upfront with all internal stakeholders regarding the projects that would be triggered by different business lines during the migration-to-cloud period. The priorities should be as much as possible agreed in advance and reflected in the Migration/ Transformation Migration Plan.

k) As the FMO services in the cloud are pretty much predefined, it is critical to first understand the CMO environment (as outlined above) and then find the most compatible CSP for the projected FMO. In that process a realistic view should be taken on what services to move to cloud and which ones to keep outside the cloud – insisting on the absolute migration of all services to cloud can be damaging for the organisation.

l) Lack of migration/transformation strategy has already been discussed above. The key message is to understand the current CMO, analyse existing CSP offerings and decide (at least) on the following:

- **i.** Is it going to be public, private or hybrid cloud?
- **ii.** Is the whole IT environment moving to the cloud or some parts stay outside it?
- **iii.** Is it going to be a single or multiple CSP (Cloud service Providers)?

m) Security mitigation is already discussed in f) above in the context of understanding CMO security environment. Once it is finished, the challenge will be to understand the cloud FMO security environment and to create a proper mapping. This whole exercise, as already indicated, would be one of determining factors for the selection of the migration/transformation strategy. In some cases the security concerns will directly trigger a decision to resort to a private cloud, or even stay outside the cloud for the part of the scope.

n) Cloud billing system is, together with the Migration/ Transformation Plan described above, the essence of the Business Plan. For each of the considered CSPs it must be analysed jointly by commercial/legal, financial and technical experts, preferably by including external consultants specialised in that area (and/or the Service Provider that would execute the migration/Transformation). Technical input is primary, it needs to describe how services would fit together. Based on it, the associated billing models need to be included in the equation in order to understand future service delivery cost.

o) Integration of services for large complex environments where multiple providers are included is always a daunting task. Knowing that, the first recommendation would be to stick to a single CSP. If there is a risk of vendor lock-in, it should be rather resolved by keeping some part of IT infra outside the cloud and potentially allocate them to another CSP in the future. Secondly, the number of third parties and Service Providers should be reduced to a bare minimum. Thirdly, there needs to be a single integrator, while the escalation point should the party that has a primary contract with a particular third party.

CONCLUSION

The introduction of cloud eliminates many risks related to the FMO environment for the simple reason that it is highly standardised and repeatedly applied to many clients.

However the migration to a cloud still comes with number of risks because the CMO non-standard architecture needs to be optimally mapped to the FMO solution and the transformation project will not be an easy ride at all. That is why the Migration-to-cloud projects should utilise all best project management practices from the previous IT outsourcing generations and combine it with the cloud-specific activities.

New World Tech
2nd Floor
Stanford Gate
South Road
Brighton
United Kingdom BN1 6SB

newworldtech.io