Cloud & Enterprise Architecture

In our new series, ‘Technically Talking’, we’ll be looking under the bonnet of new technologies. In this first article, Swaminathan Mahalingam, Technology Architect, shows how, step-by-step, The Open Group Architecture Framework (TOGAF) can be employed to guide the enterprise when moving away from a traditional on-premise solution and into the cloud.

Cloud computing is characterised by virtualised computing resources, incredible capacity and scalability, dynamic provisioning, multi-tenancy, self-service and a pay-per-use pricing model. For businesses to adopt cloud computing in a way that aligns with their business strategy, enterprise architecture (EA) is an absolute necessity.

The EA Maturity Index ranks organisational maturity levels by assigning them a score of between one and five. Interestingly, the index shows that business value is only realised when EA maturity is “standardised”. It is only at this point that cloud computing becomes a good fit.

In order to reach this point, the business will have had to define and layer the different architecture domains:
• Business Architecture
• Data Architecture
• Application Architecture
• Technology Architecture

In addition, the organisation will have well defined interoperability guidelines, identified the Internet as the target as well as the relevant cost issues. It will also have identified new product and service offerings that are in line with the firm’s strategy.

As a result of the standardised EA maturity, TOGAF Architecture Development Method (ADM) iterations should now be “cloud aware” and the enterprise architecture team will be in a position to drive the architecture development process, working collaboratively with both the business and IT.

CLOUD AWARE TOGAF ADM

The TOGAF framework provides a model and process that is capable
of incorporating both business-led and IT-led cloud requirements in a holistic framework.

**PRELIMINARY PHASE**

In the Preliminary Phase, you should consider including a strategy for the consumption and management of cloud services (public/private/hybrid clouds, semantic management, security, transactions). The governance framework will also need to include the processes and roles and responsibilities related to cloud services and operations.

At this stage, it's also important to identify the business' cloud owners from both a user and service provider management perspective.

**PHASE A**

During Phase A, you might engage in a workshop and business scenario to help you identify the business problems, the business requirements and ultimately, a potential business solution. Stakeholders in the workshop are likely to come from various business areas including: IT operations, procurement, PMO, data centre, development and CxOs.

Interoperability is an important element of this phase. The enterprise architecture team will collaborate with the business to understand and scope the needs and align them with the strategic enterprise architecture. Given the relatively low barrier to market entry, in the scenarios where the business is not sure of the viability of their proposal, it is possible to go straight to the cloud instead of "experimenting" before finalising the requirements.

At this point, there’s no turning back, so make sure that the business scenario is complete and only refer to business solutions without referring to any architecture style (as this will be discussed during Phase E) and signed off.
PHASE B
During Phase B, some variations are needed to make the business architecture cloud aware. While the overall business goals of a Software as a Service (SaaS) enabled application will not change, the business users themselves will vary within a multi-tenant scenario so this view may need to be adjusted for the different user groups. Particularly important questions to ask will be: “Who does it?” and “What do they do?” The answers will be different for cloud applications compared to traditional on-premise enterprise applications. Cloud reference models come in very handy at this stage, so it’s worth considering the following:
• IBM Cloud Computing Reference Architecture
• The Accenture Cloud Reference Model
• The Open Cloud Consortium Cloud Reference Architecture

Please note that TOGAF security activities will have to be applied to all phases, taking into account the company’s security strategy.

PHASE C
In Phase C, as in the previous phase, variations are required. The core entity relationship modeling of a cloud application may match that of its traditional on-premise enterprise application counterpart, however, multi-tenancy aspects will introduce new variations to the Logical Data Model. The process models for the data security view will be different to those for an on-premise application.

Data integration may also be an issue for cloud computing as it pushes information back into siloes to which the IT function may not have direct access. It is also worth determining the data and privacy classifications, and prioritising the risk criteria of both the data going into the cloud and that staying on-premise.

PHASE D
Within the application architecture, the Platform as a Service (PaaS) will abstract several traditional components that are part of the Application Architecture View, making this view different to a traditional enterprise application. The majority of changes will be to the technology architecture. As can be seen in the fact that concerns around the acquisition of commercial off-the-shelf hardware and software will be different for cloud architecture, when compared with its on-premise counterpart.

The nature of cloud deployment means that you will need to consider many factors including: a virtualised server environment, PaaS platform, on demand instances, dynamic provisioning of virtual storage and scalability (both vertical and horizontal).

PHASE G
In this, the Governance phase, it is worth considering the inclusion of the following activities on top of the standard ones:
• Business processes (Process-as-a-Service)
• Applications (Application-as-a-Service)
• Data (Information-as-a-Service and Database-as-a-Service)
• Technical services (Storage-as-a-Service and Infrastructure-as-a-Service)
• Security and operations implementation will have to be taken into consideration during the relocation. Security can also be considered as “Security-as-a-Service”.

The design and development team now need to be familiar with, and conform to, the Cloud API and services. This makes it easier to govern architecture usage within the enterprise. Although the enterprise architecture team hasn’t traditionally been relevant to the operational side of the organisation, this does seem to be changing with the cloud.

Ultimately this is because the common cloud management platform provides the relevant tools for management and reporting and takes away the onus of patch management, version upgrades, high availability, disaster recovery and so on.