10

TRANSITIONING TO THE CLOUD

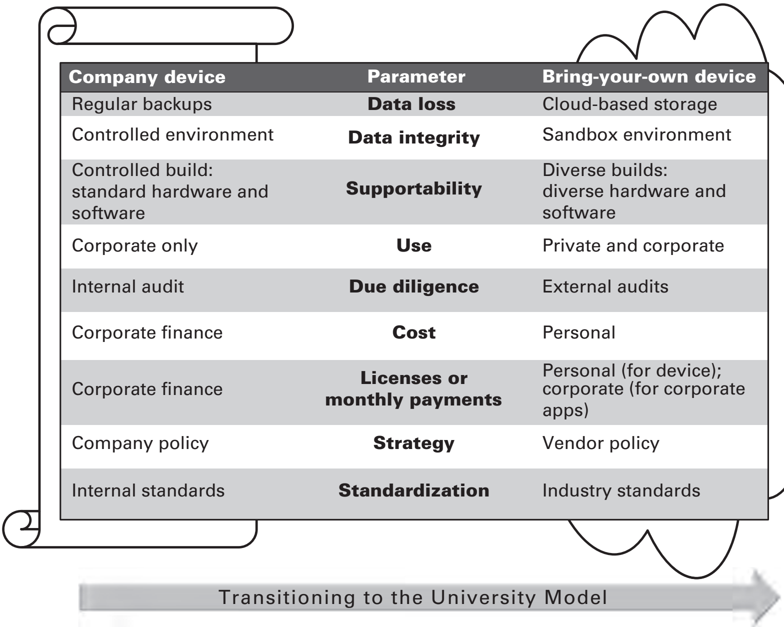
Suppose you have decided that you want to use cloud computing. What next? How will you use the cloud services? How will those services interoperate with some other cloud services from a different vendor? We consider these key aspects of using a cloud service in this chapter. Additionally, you will need to assess the cloud service vendor in terms of your SLAs so that you may select the right cloud service provider as well as the right cloud service for you. If you were to look up SLAs and metrics on the Internet or the numerous books that have been written on cloud computing, you will frequently come across a discussion of SLA metrics such as network capacity (bandwidth, latency, or throughput), storage device capacity, server capacity (number of CPUs, CPU clock frequency, and RAM), instance starting time (time required to initialize a new instance of a virtual machine), horizontal storage scalability (defined as the permissible storage capacity changes in response to increased workloads), horizontal server scalability (server capacity changes in response to increased workloads expressed as number of virtual servers in a cloud's resource pool), and the list goes on to perhaps hundreds of such items! These SLAs are good if you need to create and operate your own cloud. But why should you, as a buyer and user of cloud services, need to worry about them? After all, cloud computing is supposed to provide a layer of abstraction that should minimize your technology headache, not increase it. We will therefore not follow the well-trodden route that most books on cloud computing take. We will instead examine SLAs and metrics that are relevant to you as a user of cloud services and, additionally, provide a checklist that you can adapt to assess cloud services. After discussing these requirements, we will examine the critical success factors for a typical cloud usage model. And, finally, we will discuss how you can assess your own maturity as a cloud service user by considering a cloud maturity model from a user's perspective. This way you can assess your cloud adoption with best-practices as well as track progress over time as you use cloud computing.

University Computing Model

The university computing model, also known as the Bring-Your-Own-Device (BYOD) model, is where you have complete diversity in the device you use in order to consume IT or cloud services. Recall, from chapter 3, that it got its name because students, unlike employees at a workplace, bring their own devices to school, and universities' IT departments have had to cater to a large variety of devices. Conversely, with most businesses, there is generally some form of homogeneity in the devices used as the IT department specifies which company devices can be used.

When you incorporate cloud computing to BYOD, a paradigm shift occurs in the delivery and consumption of IT services. As figure 32 shows, a number of parameters are affected when transitioning to BYOD. And this has repercussions with a number of disciplines in the organization: from finance to company policy.

Figure 32 shows how, for a given parameter, you would need to use a different approach with BYOD. Take data loss. With a company-specified device, you would have regular backups performed as specified by the central IT department; with BYOD, the data backup should be built in to your cloud-based storage. And the cloud-based storage itself ensures that you can access that data not only from any device but from anywhere in the world. Thus the flexibility and freedom afforded to a user increases markedly. Below we consider the different cloud usage models that are applicable to a computing environment.



Company device	Parameter	Bring-your-own device
Regular backups	**Data loss**	Cloud-based storage
Controlled environment	**Data integrity**	Sandbox environment
Controlled build: standard hardware and software	**Supportability**	Diverse builds: diverse hardware and software
Corporate only	**Use**	Private and corporate
Internal audit	**Due diligence**	External audits
Corporate finance	**Cost**	Personal
Corporate finance	**Licenses or monthly payments**	Personal (for device); corporate (for corporate apps)
Company policy	**Strategy**	Vendor policy
Internal standards	**Standardization**	Industry standards

Figure 32 Transitioning to the university computing model

Cloud Usage Models

When transitioning to the cloud, you need to create a strategy[1] that considers the current, as-is, IT landscape and the future, to-be landscape, in order to create a plan of action. Generally, the IT landscape can be classified by the manner those services are delivered to you. There are five distinct usage models for the delivery and use of IT services, especially related to cloud computing. These are classified by the coupling IT has with the business. Figure 33 shows the first-generation usage model of cloud computing. This first-order usage model is based on a single IT service provider model that essentially provides services to an organization's business units with a central IT department controlling the SLAs and contracts. The single provider can appoint a third party to provide a set of services to the business units; the third party then acts as a subcontractor to the single provider. The service providers can supply a mix of services ranging from cloud computing to traditional IT.

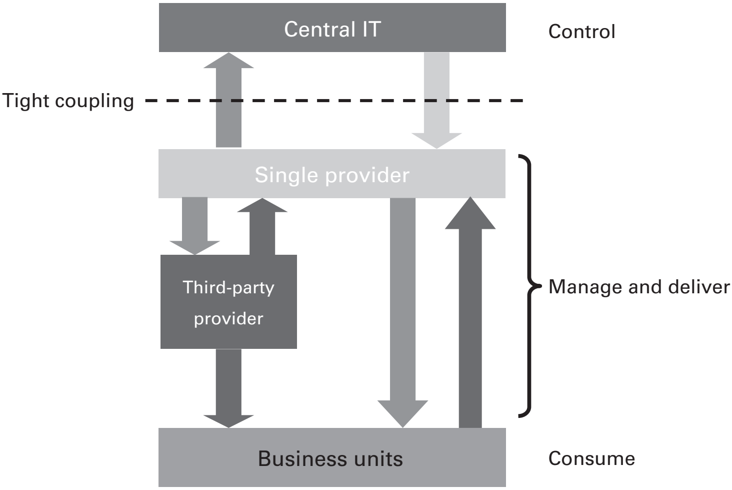


Figure 33 Single-provider usage model

The first-order usage model is the most commonly used model by organizations today. The main drawback of this model is the very tight coupling with the central IT department. This means that cloud services cannot respond in an agile manner to changing business requirements. A better model, however, is the one shown in figure 34 because it affords the flexibility to use multiple providers.

Thus, should a given provider's service not meet with changing business needs, then a different cloud service provider can be used for the needed services. The central IT department continues to act as a broker between the

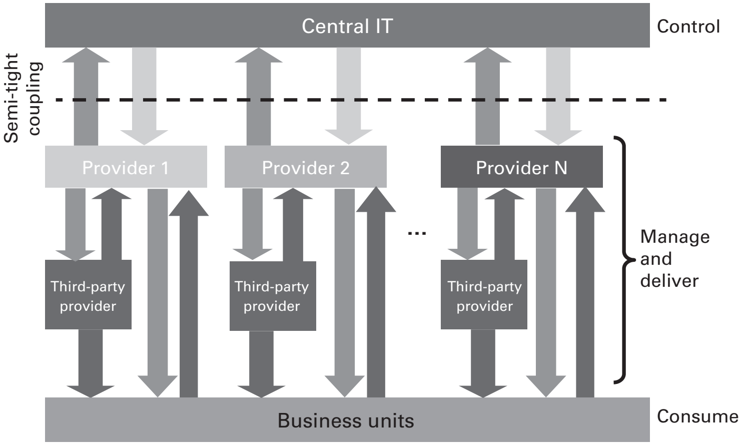


Figure 34 Multiple-provider usage model

business units and the cloud service providers. Additionally, it provides a key function—the integration of services. This integration function takes two forms: (1) to integrate the services among the various service providers, and (2) to integrate the business units with the providers. Although most organizations purport to use this model for IT services, whether or not related to cloud computing, they usually do not have such a model implemented because of the often insurmountable challenges that the central IT department faces in performing the integration function. One possibility is to appoint a service integrator (not a systems integrator!) to perform just such a function, as figure 35 shows.

The role of service integration is to ensure that a portfolio of IT products and services meets business needs in a consistent and efficient manner. The central IT department does not engage with the cloud service providers in such a model but works directly with the service integrator. Optionally, the service integrator could manage the contracts, reporting, and billing functions with the cloud service providers individually and then provide a consolidated report and bill to the central IT department. With this usage model, there is considerable flexibility for the business units to receive cloud services from three different parties: (1) the service integrator, (2) a third-party provider that the service integrator appoints, and (3) other service providers that the central IT department appoints. All these

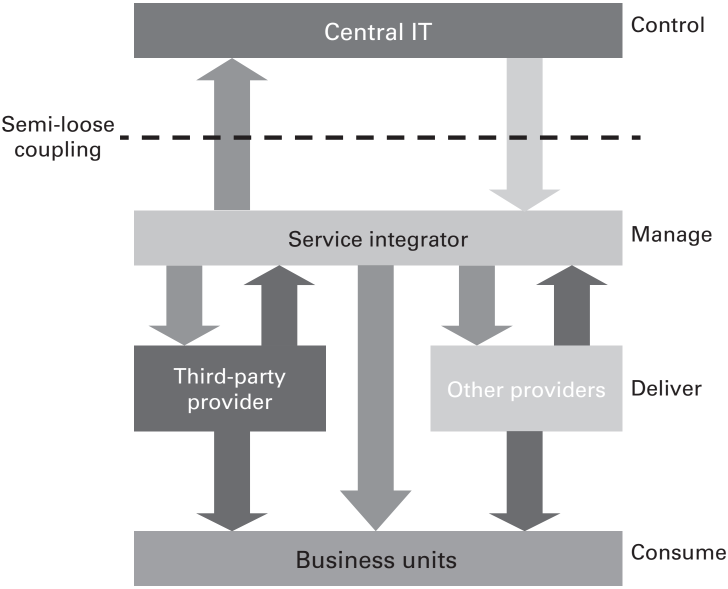


Figure 35 Third-order usage model with a service integrator

appointees provide services to the business units, with the central IT department still maintaining overall oversight of the cloud services on behalf of the business. But there still remains a problem over shadow IT,[2] and this problem is compounded greatly due to the convenience and flexibility afforded by cloud computing. One of the major issues that shadow IT opens up is an increased vulnerability to security breaches resulting from the nonstandard approach to IT taken by the business units. On the other hand, the reason why business units resort to shadow IT is because the usage models discussed so far lack the agility to meet business demands in a timely manner. A usage model that addresses these issues is therefore required; its main characteristic is to have loose coupling between the central IT department and the cloud service providers as figure 36 shows.

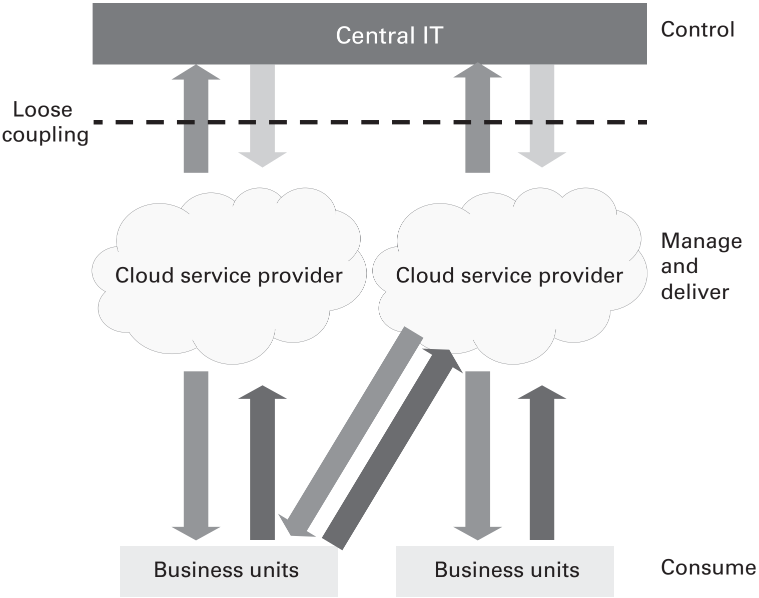


Figure 36 Service delivery based usage model

The usage model of figure 36 is distinct from the usage models previously discussed because its purpose is to especially address cloud services natively. The previous models were predicated on the use of traditional IT services or private cloud services. With the service delivery based usage model of figure 36, the central IT department maintains a catalog of cloud services and cloud service providers from which the business units can choose; the business units engage directly with the cloud service providers in terms of the billing and SLAs. The central IT department then subsumes the role of the service integrator. As the adoption of this model evolves in the workplace, and traditional IT is eventually replaced by cloud computing, the role of central IT should evolve to a distributed, rather than a central, function as figure 37 shows.

Having a distributed IT function embedded in the business units makes the business much more agile and able to fully exploit the advantages of cloud computing. The IT function would then be led by a chief technologist who would be responsible for defining the standards within the organization to engage with the cloud service providers. Secondarily, his role would be to provide governance and auditing in order to ensure that the services and the business units follow the defined technology standards. The other, traditional, functions of the central IT department such as billing and IT contract management simply become incorporated with the finance and procurement departments, respectively. It

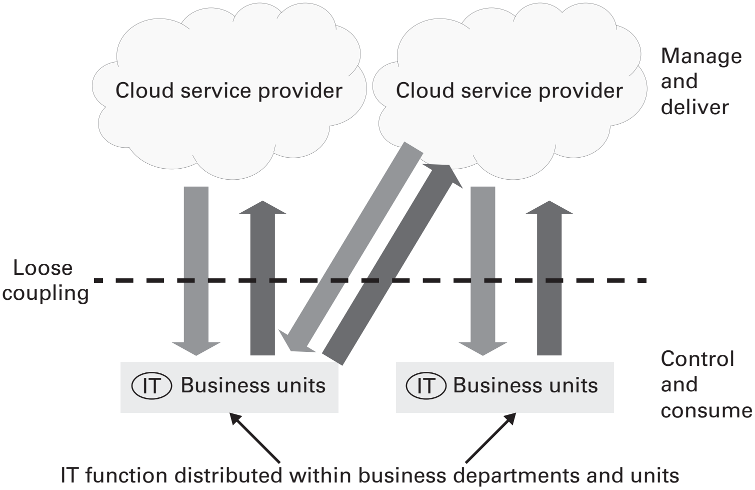


Figure 37 Service consumption based usage model

is this minimalist vision of IT that cloud computing enables. And that is one of the main reasons why cloud computing presents such a paradigm shift for the workplace and businesses in general: it devolves the control of IT from a select few residing in a central IT department to the many users of IT within the business departments!

Interoperability

As you will have gathered from the previous discussion, each of the usage models we considered had an underlying common principle: for every service to coexist with another. In addition, for business continuity or commercial reasons, you might also want to ensure that a cloud service can be replaced by a similar one from another provider. All this calls for interoperability between services.

Interoperability is the capability to use the same or similar cloud services offered by different cloud service providers.

The scope of interoperability does not extend only to technical matters, but also to such topics as the integration of billing, reporting, management, business processes, and, of course, data. And this is regardless of the cloud delivery model used—private, public, hybrid, or community. The following section heads constitute a checklist that you can adopt and extend to ensure that your cloud services have interoperability.

Governance and Auditing

If you are using an auditing process and policy for one cloud service, then you should ensure that any other services you procure to interoperate with your current cloud service also conform to that same auditing standard. Similarly, for governance, you need to ensure that the same governance board within your organization has oversight of all the cloud services, especially those that need to meet interoperability requirements.

Compliance

If you need to comply with industry or countrywide regulations, then you should establish whether the cloud services you use come under their scope. If they do, then all the cloud services that need to interoperate have to comply with the same regulations. Generally, from a cloud services perspective, there tends to be a gradation between general regulations and industry-specific regulations as the cloud service becomes more specialist in nature. This is shown in figure 38 where general, utility, services like email and office productivity have global scope and a requirement to abide by general, international, laws and regulations. When more specialist cloud services are considered, local

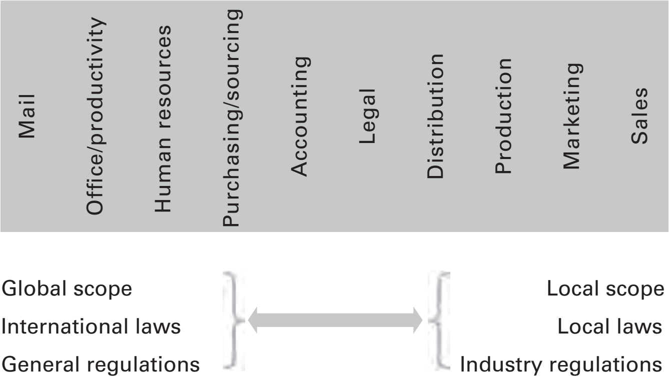


Figure 38 General compliance requirements

laws and industry regulations normally apply. This is a general observation that may not always apply to a specific cloud service, however.

Security and Data Integrity

For data integrity, the same encryption standards and schemes need to be in place across the cloud services that need to interoperate. Otherwise, data flow will not occur seamlessly. For security, you will need to ensure that the same security procedures are in place in order for there not to be a disparity in the security levels between the interoperable cloud services. You should also ensure that the users of all the services have common security training because it is best to standardize on a single security policy within an organization.

Data Integration

For seamless data integration between cloud services, two factors are important: a common format and a common data model. Format refers to the way data are presented; a spreadsheet stores information in a different format to a text file, for instance. Even when you have the same format, there needs to be commonality about what the data relates to. For example, if you have two text files (notice that both have the same format) but one file contains information about your inventory whereas the other one contains information about your salary, then both have dissimilar data models. So you need to ensure that the cloud services that interoperate use the same data format and models.

Process Integration

Besides having the same data format and model for interoperability, you need to ensure that tasks are carried out by the cloud services for the same business process. This is process integration. There are two aspects to process integration. One is where you want one process in a cloud service to receive data from another and commence a workflow that is an extension of the first process; the other aspect is when you want both processes to be the same so that you may interchange them, almost in a plug-and-play manner. For both aspects, you will need to ensure that the processes use the same business process language (BPL) and protocol in order for your cloud services to be interoperable. To make things easy with data and process integration, an enterprise service bus (ESB) is usually used to ensure that many of the technical integration concerns are hidden at a lower layer of abstraction.

Business Continuity

There are two aspects to business continuity. One is related to disaster recovery where you would want to use a secondary cloud service, most likely from a different service provider, in order to ensure that minimal disruption to your cloud service. Another aspect concerns the need to use a secondary cloud service provider in case the current one cannot meet a spike in your capacity demand. Both aspects can use cloud bursting to ensure seamless flow of control from one cloud to another. However, the capability to use cloud bursting or some such automated method of using a similar cloud service between different vendors needs to be in place. This is much more a technical requirement that uses the right protocol and standards to ensure that control passes from one cloud service to another seamlessly. In addition, it is likely that data and process integration requirements shall have to be met in order to permit business continuity.

Monitoring and Alerting

In the future, cloud services are expected to become self-healing in that the monitoring and remediation processes will become automated. But until that happens, you need to ensure that any alerts arising from the monitoring of your cloud services use a common standard and format for communication to your team. This way your team will be able to respond to the alerts in a timely manner. You can also be proactive here by performing certain tests on a regular basis. These tests could be, for example, stress tests to ensure that you have the right capacity for serving your customers or penetration tests to assess whether any security gaps exist that might result in a security breach.

In the future, cloud services are expected to become self-healing in that the monitoring and remediation processes will become automated.

Billing and Reporting

The billing processes, formats, and reports (I am using this generically to denote statements and invoices) should all be similar between the services in order for you to assess their total cost of ownership in a meaningful and rapid way. You may also need to ensure that the people that work with billing have a common understanding of the processes and reports in order for you to have interoperability not only with the processes and reports but also with people.

Business Processes

Transitioning to the cloud gives you a good opportunity to re-design your business processes in order to make them more efficient. Processes connect different parts of a business and so improving them should improve your whole business. And cloud computing can be an excellent enabler in re-engineering a business because of the automated business processes that you can have using a BPaaS cloud. Even if you do not go all the way to BPaaS, you can still derive greater efficiencies in your processes through the onboarding of INaaS and SaaS cloud services—and thereby effect business change.

The business process re-design (BPR) model (created by Hammer and Champy) shown in figure 39 provides a good procedure for re-designing your business processes.[3] The main idea in adopting the BPR model is that attempts

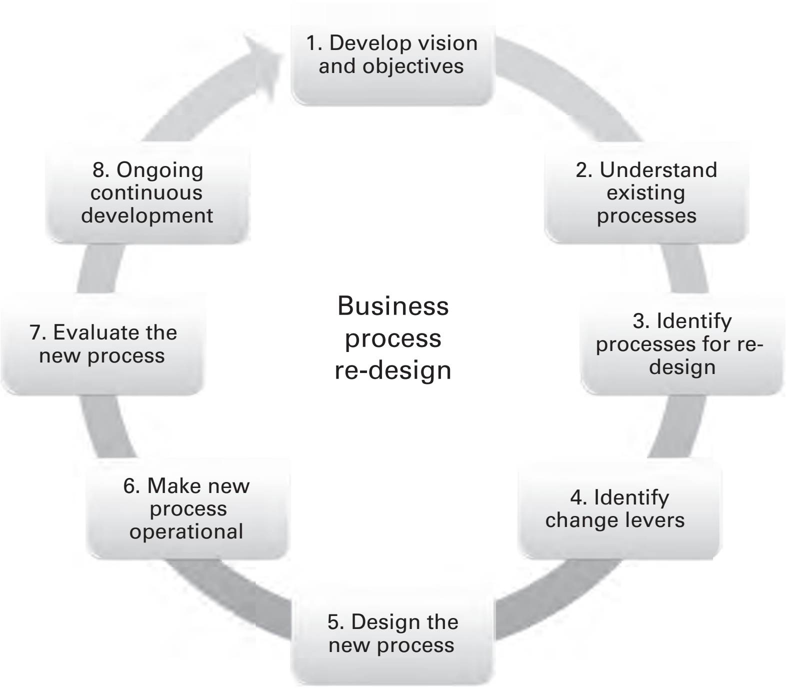

1. Develop vision and objectives
2. Understand existing processes
3. Identify processes for re-design
4. Identify change levers
5. Design the new process
6. Make new process operational
7. Evaluate the new process
8. Ongoing continuous development
Business process re-design

Figure 39 Business process re-design model

to improve the efficiency of organizations can only succeed if the processes are also improved. (This also applies to IoT related processes as the machine to machine interactions need to be similarly efficient.) Thus, when using the BPR model, one of the questions asked (during step 3 of figure 39) is whether a process, or one of its workflows, is necessary. Only those deemed necessary are kept, improved, and implemented. At step 5, you will design some of the processes as BPaaS cloud services in their entirety, some as using one of the cloud service models, and others outside the cloud. The criteria that you use to assess whether a service ought to have a cloud computing component are defined by your requirements and critical success factors, which we outline next.

Requirements and Critical Success Factors

When transitioning to the cloud or considering a new cloud service, you will need to have a set of requirements that will provide you with a yardstick for comparing cloud services. Additionally, the requirements will help you to crystallize your SLAs so that you may assess whether a cloud service is appropriate for you. Remember, cloud computing does not fulfill all your IT or computational needs; there will be instances, such as where very high-speed computing or resilience is needed, when you will want to use traditional computing. Given below is a checklist that can help you define your requirements for cloud computing. You can also use the requirements to define the critical success factors for the cloud services that you purchase. I have classified them into three categories: functional, non-functional, and business-related requirements. They are generic enough for you to use them for all the deployment and service models of cloud computing.

1. Functional requirements
    - Maturity
    - Interoperability
    - Feature-set
    - Usage model
2. Non-functional requirements
    - Security
    - Availability
    - Resilience
    - Network capacity
3. Business requirements
    - Price and value models
    - Risks
    - Business continuity
    - Support model
    - Reporting and billing

You can create a score matrix by scoring each of the requirements from, say, 0 to 3, with 0 denoting that a requirement is not met and 3 denoting a requirement being met entirely. Also each requirement could be weighted to reflect what you consider to be most important. For instance, maturity might have a weighting of 0 if that requirement is not at all important to you, but resilience might have a weighting of 3 to denote its high importance. Multiplying the weighting with the score will then provide you with a weighted rating for that particular requirement when comparing cloud services or their vendors.

Cloud Maturity Model

Figure 40 shows a maturity model for cloud computing. It has five levels of maturity: performed, defined, managed, adapted, and optimized (the highest level of maturity). The primary two rows of the table, titled "focus" and "success factors," describe the level of maturity in terms of its main characteristics and benefits, respectively. The last five rows consider the maturity characteristics of your cloud service in terms of (1) the people engaged to purchase, use, and manage the cloud services; (2) the processes that interact with the cloud services; (3) the financial and usage monitoring and reporting of the services; (4) the security, regulatory, functional and financial oversight that is provided

Maturity level	1. Performed	2. Defined	3. Managed	4. Adapted	5. Optimized
Focus	Functional; meets business needs on an ad hoc basis	Competent in saving costs and securing assets	Effective in alignment to business needs	Responsive to business needs	Automated business functions
Success factors	New (or consolidated) business processes	Cost effective due to standardization	Agile, flexible, and reduced time-to-market	Measurable and repeatable outcomes	Continuous improvement built in
People	• No team in place • Little or no knowledge of cloud computing	• Basic roles and responsibilities defined	• Regular training in place • Roles and responsibilities being practiced	• Knowledge management in place • Incentives for cloud service reuse in place	• New optimized cloud services implemented
Processes	• No interoperability standards defined • Cloud service reuse and life cycle not defined	• Data and process interoperability defined • Best practice defined • Service life cycle defined	• Cloud service reuse being evangelized • Data and process interoperability in place	• BPR model followed • Business activity monitored for key processes	• Agile and optimized processes in place • Business processes continuously improved
Monitoring and reporting	• No or minimal monitoring • Reporting mostly relegated to billing	• Metrics and KPIs defined	• Metrics and KPIs reported	• Metrics and KPIs tracked	• Metrics continuously optimized to meet business needs
Governance	• No clear ownership of the cloud service	• Ownership is defined • Sponsorship from top management	• Governance process defined and followed • Communication plan in place	• Metrics and KPIs governed across all business units	• Federated governance with all business units in place
Financial control	• Usually based on credit cards	• Billing and related utilization statements tracked	• Penalties and chargebacks defined	• Financial planning and budgeting in place for use of cloud services	• Cloud computing considered a profit center as it becomes part of the business model

Figure 40 Cloud maturity model

to ensure that the cloud services meet your needs; and (5) the financial management in place to ensure that the cloud services remain financially viable. The maturity levels are not mutually exclusive for these five characteristics; you can have a maturity level of 1 for people and a maturity level of 3 for processes, for example. However, the overall maturity of your cloud service would be denoted as that level at which most characteristics coincide.

You can use the maturity model in two ways: first, to create a strategy to improve your use and commissioning of cloud services—this will enable you to transition from one maturity level to a higher one; second, to understand best-practice cloud computing. Obviously, the final column, describing the optimized maturity level, should be considered as the ultimate goal.