OPEN DATA CENTER ALLIANCE℠ MASTER USAGE MODEL: BUSINESS STRATEGY ENABLED BY CLOUD REV 1.0

TABLE OF CONTENTS

CONTRIBUTORS

Ray Callus – National Australia Bank
Pankaj Fichadia – National Australia Bank
Eric Hamer – Intel Corporation
Christoph Jung – T-Systems
David Klein – National Australia Bank
John Pereira – Intel Corporation
Ryan Skipp – T-Systems

LEGAL NOTICE

OPEN DATA CENTER ALLIANCE℠ MASTER USAGE MODEL: BUSINESS STRATEGY ENABLED BY CLOUD REV 1.0

EXECUTIVE SUMMARY

Cloud computing has been posed as an ideal solution to assist businesses in achieving their computing objectives. Cloud computing can offer IT services on demand with the following benefits:

- Ability to scale to meet business demands in real time, paying only for what is used
- Cost benefits derived from critical mass for processing and operations levels, operated by experts in their fields, with shared development costs

However, several considerations must be dealt with before these benefits can be sustainably recognized. These considerations include preparing existing teams and systems to work with the cloud, creating rules that control what data can be stored where, and deciding how risk and legislative requirements will be managed and delivered. Investment is also necessary in the areas identified in this document to prepare the organization to be able to best leverage cloud-based services and successfully and consistently report achieving the expected advantage. Also, control and governance must be defined to mitigate the risk of business units bypassing internal IT, procurement, and risk processes.

If these controls are not in place, the risk arises of a "shadow IT" organization forming, consisting of alternately sourced IT services from outside the IT organization and infrastructure, which potentially can lead to compliance and control gaps for an organization, along with possible leakage of intellectual property and data.

The Open Data Center Alliance (ODCA) recognizes and strongly promotes the need for organizations to develop a clear, well-defined, and well-communicated cloud strategy for their business units. The ODCA has identified various dimensions that we recommend be addressed in such a strategy. These dimensions are mostly encapsulated within the ODCA Cloud Maturity Model (CMM). On its own, though, the CMM is not sufficient. A written strategy must also be articulated, which is specific to a business and aligns to the organization's unique business objectives and strategic and operational requirements.

This document represents a usage model for guiding the creation of a business strategy enabled by cloud-based services. It identifies the key considerations that should be taken into account when developing a business strategy for cloud adoption and business transformation.

This document serves a variety of audiences. Business decision makers looking for specific frameworks and enterprise IT groups involved in planning, operations, and procurement will find this document useful. Solution providers and technology vendors will benefit from its content to better understand customer needs and tailor product and service offerings. Standards organizations will find the information helpful in defining standards that are open and relevant to end users.

A number of key areas are identified in this document. An organization's cloud strategy should adequately address these areas, always in the context of the actual business, its practical needs, and the strategic positioning of the business. Each section identifies some of the important concepts, considerations, and typical approaches or methods potentially applicable in that category.

By defining a cloud strategy that comprehensively addresses these areas of cloud adoption and integration, the result should be a referenceable document that is useful to pragmatically guide the various organizational units and projects in setting priorities, making decisions, and selecting options and solutions to challenges.

TAXONOMY

Table 1 lists the standard terms and definitions used in this document.

Table 1. Terms and definitions.

Actor	Description
Cloud Consumer	An individual in a cloud subscriber organization that is using one or more cloud-based services.
Cloud Service Provider	An organization providing cloud services and charging cloud subscribers. A cloud provider offers services over the Internet. A cloud subscriber could be its own cloud provider, such as for private clouds.
Cloud Subscriber	An organization that has been authenticated to a cloud and maintains a business relationship with a cloud.
Solution Provider	A technology vendor selling technology elements that can be used to build a cloud or other service, usually specializing in either a specific software product, a specific hardware product, or possibly by providing consulting services.

ANCHORING A CLOUD STRATEGY WITHIN A BUSINESS CONTEXT AND BUSINESS MATURITY EXPECTATIONS

The cloud strategy does not exist in a vacuum. It needs to identify how cloud technology can enable the organization to achieve its business goals, which must be in the context of how the organization consistently measures and reports ongoing progress toward achieving those goals. Similarly the cloud strategy should reflect what cloud maturity level the organization wants to achieve. The following sections discuss these considerations and present a formal usage model for adopting cloud-based services.

Alignment with Business Goals

Conceptually, one can either bring cloud to the enterprise or bring an enterprise to the cloud. The former generally applies to large-scale and legacy enterprises, and the latter generally to startups. In either case, a strategy relating to the use of a technology should always reflect the business goals of an organization. It is also important to stipulate how the organization will measure the way in which cloud-based services contribute to this achievement. These metrics enable organizations to define targets and track progress.

In the context of cloud technology and services enabling business transformation, the primary measurements or metrics typically relate to the following:

- **Efficiency.** Cost improvement of operations
- **Velocity.** Agility to quickly adopt or support new functions and capabilities for the business
- **Time.** Scaling of capacity to match business requirements directly (just in time)
- **Focus.** Enablement of human resources to focus on business needs
- **Capability.** Flexibility of existing solutions to be cost effectively reused to enable new initiatives
- **Quality.** Improved quality through use of specialized resources, processes, and facilities
- **Reliability.** Highly available solutions and infrastructure

The process for developing a cloud strategy for business transformation therefore could be as follows:

1. Identify and list the business goals and how they are measured and reported at the corporate level.
2. Identify the organization's short-, medium-, and long-term objectives toward the attainment of those goals.
3. Identify which of the objectives in step 2 could be enabled or further transformed by cloud services or technology concepts.
4. Identify how the achievement of business objectives can potentially be improved and transformed through the use of cloud-based services.
5. Identify any relevant data privacy or data protection obligations that apply because of public law or other regulations.
6. Determine appropriate measurements to apply against each business objective in the context of the business benefits. Then identify appropriate areas of activity relating to business goals and how cloud-based services affect that activity. For example, a company could measure the time necessary to release a new business product, when cloud technology is used as an enabling technology and the business objective is to release "x" number of new products to market, per annum.
7. Proceed with detailed planning and implementation for the adoption and integration of cloud services in the identified areas.
8. Track progress and results.

All measurements should relate to the fundamental criteria associated with achieving the business goals. This approach is often called the SMART approach:

- Specific
- Measurable
- Achievable
- Realistic
- Time bound

Nearly every cloud solution has a functionally equivalent non-cloud alternative, although its service and commercial structure may differ from the cloud version. Therefore careful analysis of the opportunities that cloud-based services represent is necessary when developing an organization's cloud strategy. This analysis will help avoid the "future legacy" syndrome, where a technology is considered shiny and new at first, but because of a lack of strategy becomes ineffective in a few years.

Cloud technology offers significant potential to enhance agility, increase adaptability, and reduce costs. Cost reductions typically are achieved by avoiding unnecessary service capacity or even entire data centers. These three benefits—agility, adaptability, and cost efficiency—are the key ones to map toward enabling business objectives. By using these benefits, an organization transforms to a cloud services broker that orchestrates cloud-based services according to its business needs. However, certain enablers from the business side must also be established before the benefits can be fully achieved (as described in the Key Enablers section).

Cloud Maturity Level

An important aspect of defining the strategy is to determine what degree of maturity the organization wants to achieve. The target maturity level determines how the organization invests in various key enablers of effective cloud-based service adoption. As with any maturity model, the appropriate cloud maturity level depends on the business focus, type, industry sector, and other factors. It is NOT always necessary to aim for maximum maturity levels in all aspects, as these may not be affordable, or a higher maturity level may not contribute to enabling the business any more than a lower level might.

The ODCA realized that most CMMs focus on particular technology-related aspects of the cloud and not the whole stack of enablement, including business levels. Therefore, the ODCA has developed a model for demonstrating cloud maturity and capability, not just at a technology adoption level but also at an enablement level, from the lowest technology layers right up into the business (for more information, see the ODCA Usage Model: Cloud Maturity Model Rev 2.0[1]). This CMM model helps organizations to understand key enablers for adopting cloud-based services and plan the appropriate activities, budgets, and resourcing to get to the desired state.

Each organization should strongly consider working through the various layers of the maturity model (from technology infrastructure all the way up into business), define what their target capability state should be per area against a defined timeline, and allocate a focused investment budget to achieve that capability state. This process should of course always remain appropriate to the nature of the business. For example, it may not be necessary for a company in the baking industry to require real-time federated services with full automated processes and workflows. This approach would simply be an over-investment in unneeded, inappropriate capability. The same holds true for the service quality levels: choose the appropriate ones for the business requirements.

[1] www.opendatacenteralliance.org/library

The ODCA identifies service characteristics for cloud-based service elements in two classes: quality and maturity. Tables 2 and 3 describe these classes.

Table 2. The characteristics of quality service.

	Cloud Service Quality Level			
	Bronze	Silver	Gold	Platinum
Description	Represents the lower-end corporate security requirement and may equate to a higher level for a small to medium business customer	Represents a standard level of corporate security likely to be evident in many enterprises	Represents an improved level of security that would normally be associated with the processing of sensitive corporate data	Represents the highest level of contemplated corporate requirements
Example	Development environment	Test environment; "out-of-the box" production environment	Finance sector production environment	Special purpose, high-end security requirement (for example, military)

Table 3. The levels of the cloud maturity model (CMM).

	Cloud Service Maturity Level				
	CMM 1	CMM 2	CMM 3	CMM 4	CMM 5
Description	Initial	Repeatable	Defined	Managed	Optimized
Result	Initial efficiency gains	Capability gains	Efficiency gains	Increased velocity, increased quality	Cloud-based systems aligned to and enabling a proactive business strategy

In addition, maturity is divided into two capability level groupings: business- or enterprise-level and technical level.

Business- or Enterprise-Level

- Business's Organizational Units
- Human Resources
- Procurement
- Finance
- Risk Management
- Project Management

Technical Level

- Information technology
- Application development
- Architecture
- Security
- Technical cloud services that are incorporated, including:
  - Infrastructure as a service
  - Platform as a service
  - Software as a service
  - Data as a service

After assessing maturity requirements and the current environment, the organization should, in alignment with the scope and nature of the business, define a target maturity level for each requirement. The next step is to plan activities to close the gap between the current status and the target status. This plan should include resourcing for those activities, a timeline, and a budget.

Here is an illustrative example: Many organizations are starting with an enterprise private cloud and then extending the model to public cloud, taking advantage of public clouds for specific use cases. One of the reasons to choose this strategy is to address organization and technology maturity; the organization doesn't have to extend legacy environments. Suppose risk management requires an online cloud data landscape view in real time, to be able to determine and manage threats actively (that is, CMM level 4/5). Also suppose that this CMM level is appropriate to the business sector in which the organization resides. In that case, monitoring and deployment tools will need to be built, control processes

implemented, and policies, rules, and guidelines defined. Moreover, all of these must be integrated into the organization's cloud service orchestration work packages and workflows so that compliance is automatically built into every deployment from the beginning.

This project would be undertaken with the usual project parameters assigned to it as described in the previous paragraph. Of course, many of these parameters may already be in place for non-cloud based systems. The primary difference is that they may have to be extended to work with (potential) external cloud providers and operate in real time, since the cloud concept is for a real-time service. In contrast, most traditional internal IT environments are based on batch-run systems, which may report only daily.

For each of the described maturity levels, a matrix may be determined, with a target rating and actions to close it. Table 4 describes such a matrix, with a separate set of activities for each identified capability.

It is valuable to understand the ODCA rating for business strategy in the context of the CMM, as shown in Table 5, on the next page.

Table 4. Sample matrix for planning cloud maturity level (CMM) activities.

	Maturity				
	CMM 1	CMM 2	CMM 3	CMM 4	CMM 5
Bronze	Describes the characteristics of this quality level				
Silver	Describes the characteristics of this quality level				
Gold	Describes the characteristics of this quality level				
Platinum	Describes the characteristics of this quality level				
Action plan to graduate to next CMM level	Describes the actions to get from this to the next CMM level				

Table 5. ODCA rating for business strategy in the context of the cloud maturity model (CMM).

	CMM 1	CMM 2	CMM 3	CMM 4	CMM 5
Typical CMM-Level Characteristics	• Mapping and analysis of cloud potential for existing systems and services. • An awareness of cloud computing has been established, and some groups are beginning to implement elements of cloud computing • There is no cohesive cloud computing plan being followed.	• An approach has been decided upon and is opportunistically applied. • The approach is not widely accepted and redundant or overlapping approaches exist. • May be informally defined, or if documented, may exist primarily as "shelf ware." • Initial benefits of leveraged infrastructure. **Capability gains**	• The affected parties have reviewed and accepted the approach. • There has been buy-in to the documented approach, and the approach is always (or nearly always) followed. **Efficiency gains**	• The capability is being measured and quantitatively managed through some type of governance structure. • The appropriate metrics are being gathered and reported. **Increased velocity, increased quality**	• Metrics are consistently gathered and used to incrementally improve the capability. • Assets are proactively maintained to promote relevancy and correctness. • The potential for market mechanisms to be used to leverage inter-cloud operations has been established. **Cloud-based systems aligned to and enabling business strategy, proactively**
Activity Plan to Move Organization to Next Maturity Level	• Develop a corporate strategy for incorporating cloud services into the business landscape. • Develop application and data classification frameworks and policies relating to security, compliance, and risk management. • Define data protection policies, guidelines, and rules, per application class.	• Develop a set of measures against the business objectives and goals, for how services are achieving those goals. • Create a cloud service adoption plan with milestones, activities, and a timeline. • Create a communication plan to the business that informs and educates about the incorporation and positioning of cloud services. • Create a training plan to address skills and culture changes and the evolution needed to successfully adopt and enable cloud service adoption.	• Define an incentive scheme against the achievement of business objectives, relating to cloud service integration.	• Define targets numerically against each of the business objectives and integrate them into the cloud service portal and orchestration system.	
CMM Control Set Resulting from Activity Plan	• Ad hoc cloud service adoption with different frameworks and classifications of requirements.	• A written and communicated corporate strategy exists that aligns cloud-based services and business objectives. • A classification framework for all business applications and data exists with all apps considered for cloud classified. • Defined data classes exist, with rules, policies, and guidelines communicated to the organization.	• Well-defined measures exist for the attainment of business goals and objectives, and services are reported in this context. • A cloud service adoption plan exists, with milestones defined, planning, and budget. • A communication plan exists relating to cloud services, and detailed follow-through activities with the impacted business units is ongoing, including a feedback mechanism, and regular progress reports, possibly through corporate communications vehicles. • A training and development plan exists and is implemented, defined per impacted business unit.	• An incentive scheme exists and employee measurement (where appropriate) aligns to the achievement of this strategy.	• Systems are automatically deployed in context of the business objectives.

Usage Scenario: Adopt Cloud-based Services to Enable Business Transformation

Goal

The overarching goal is business transformation, and technology enablers are needed to enable that transformation. Cloud technology offers many of the transformational capabilities required to compete in the future marketplace, and the organization needs to create a structured plan for the identification, assessment, migration, integration, and management of cloud technology.

Assumption 1

The organization recognizes the potential value that cloud-based services could deliver.

Assumption 2

There is executive-level sponsorship and commitment.

Success Scenario 1

A clear strategy is established that addresses the necessary dimensions of cloud-based services required to enable business objectives and transform the business. Using project-based delivery, cloud-based services are integrated with the business and deliver the expected benefits to the various business sub-units.

Failure Condition 1

Impacted business units do not align with, participate in, or adopt cloud-based services according to the defined cloud strategy, thereby diluting the overall benefit realization, cloud investment, and integration of cloud-based services. Additionally, ad hoc business units independently adopt cloud-based services outside of the planned governance structures, and control is lost across the entire IT, commercial, risk, and data landscape. Cloud initiatives are isolated and do not add to organizational drivers of business enablement, velocity, transformation, and effectiveness.

DECIDING WHAT AND HOW TO MOVE TO THE CLOUD

Adoption of cloud-based services presents many choices. Depending on the organization's business goals, it may be appropriate to move some business systems and applications to the cloud, but not others. In the same way, certain categories of data may be good candidates for cloud-based services, while other data should be kept on-premises. Organizations must also choose a service model and cloud deploy options that meet the organization's objectives. This section discusses each of these decision areas in further detail.

Two important aspects of categorizing business systems, applications, and data include the following:

- **Differentiating capabilities.** A competitive capability in terms of how the organization competes in the marketplace. For example, design engineering—how the company makes its product—is a differentiating capability.
- **High-risk data.** Data with a high security rating, normally involving intellectual property and/or regulatory requirements.

Figure 1 illustrates some resulting considerations from these initial factors.

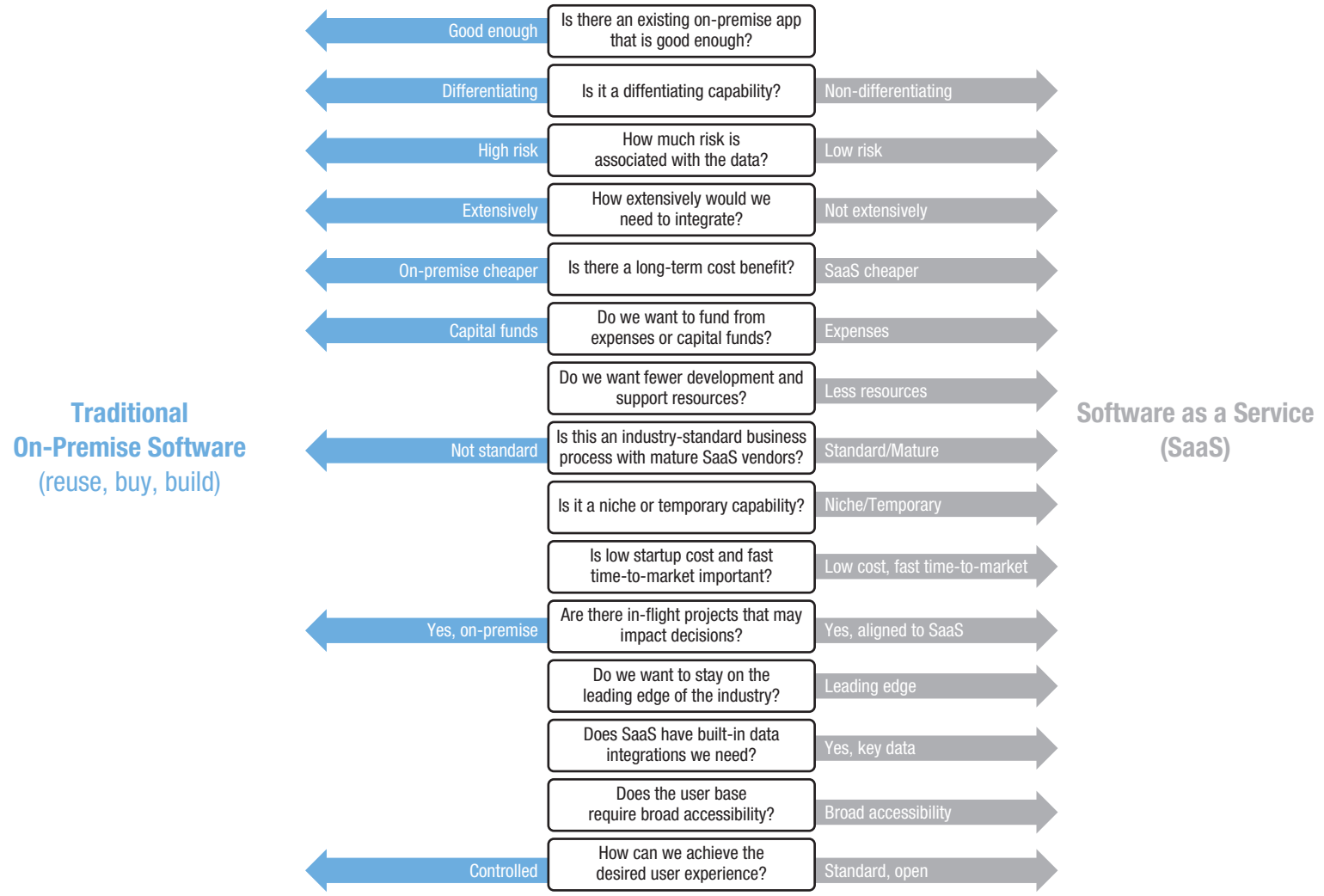

Figure 1. How differentiating capabilities and high-risk data affect adoption of cloud-based services.

Business Systems and Application Categorization

Not all business systems or applications are suited for the cloud environment. And, even for those that are, decisions about governance, cloud service provider selection, and other considerations can differ from one business system or application to the next. This section describes a categorization method that can help organizations determine what should be moved to the cloud and how.

Business Systems

As shown in Table 6, the systems that support a business can be categorized into four major groups: mission critical, core, essential, and important. Further subdivision is then possible, which usually relates to the intellectual property of the business that resides within those systems and the criticality of the data that they contain.

Table 6. Categories of business systems.

Category	Exhibits Most of These Characteristics
Mission Critical	• Critical to the health or safety of employees, clients, and partners • Will threaten the ongoing viability of the organization and/or its reputation if service is compromised for more than 1 to 4 hours • Will cause major legal, compliance, or regulatory ramifications if service is compromised for more than 1 to 4 hours
Core	• High chance of threatening the ongoing viability of the organization and/or its reputation if service is compromised for more than 4 hours • High chance of major legal, compliance, or regulatory ramifications if service is compromised for more than 4 hours • Critical component in providing academic, administrative, or medical operations • Outage impacts more than one area or system
Essential	• Chance of threatening the ongoing viability of the organization and/or its reputation if service is compromised for more than 1 day • Chance of major legal, compliance, or regulatory ramifications if service is compromised for more than 1 day • Generates daily financial revenue equal to or greater than "$x" (business to determine actual number for itself in its context) • Outage impacts more than one area
Important	• Chance of threatening the ongoing viability of the organization and/or its reputation if service is compromised for more than 5 days • Chance of major legal, compliance, or regulatory ramifications if service is compromised for more than 5 days • Adds capability or value to a mission-critical system as a dependency

Business Applications

Organizations should also determine the cloud positioning of business applications, in the context of their interaction with important parties. There are three main types of business applications:

- **Business to customer (B2C).** These are generally browser-based, customer-facing applications, including dynamic content-based web sites. Examples include ordering systems, customer support systems, web sites providing product information, applets and Active-X lightweight clients, and clients that are installed on customer end-user devices.
- **Business to business (B2B).** These applications are used between business partners, such as suppliers and resellers. Traditionally these applications are accessed using dedicated links between business partners. Many of these applications also use the Internet with security features such as virtual private networks (VPNs). Examples include parts ordering and status systems and bulk order submission web services.
- **Enterprise.** These applications are used within the organization (intranet) where the users are primarily enterprise workers, and the applications are not exposed or available outside the enterprise to external parties. These include both web-based applications and desktop applications. Examples include human resource systems, internal financial and enterprise resource management systems, IT desktop support systems, email clients, and instant messaging. These applications are becoming increasingly Internet-facing because most enterprises are allowing employees to bring their own devices into their work environments.

Using a Matrix to Categorize Business Systems and Applications

It is often easiest for companies to consider all of their systems critical, especially when left to a democratic vote by combining the input of all the various business units. In reality and from an executive perspective, this is not usually true. Many workarounds may enable a business to continue operation in the absence of a specific system, enabling that system to be relegated to lower importance.

Categorizing business systems and applications offers an organization a clear view of which systems are important enough to protect by investing technologies such as high availability, disaster recovery, encryption, and increased security monitoring. Since these technologies can effectively duplicate the IT costs of the organization, thereby pushing up production and operating costs significantly, it makes sense to prioritize, invest, and

manage systems appropriately and as cost effectively as possible. Figure 2 shows a matrix for prioritizing systems, where each system is scored against or positioned within the matrix, and a potential cloud-related positioning is thereby created.

Figure 2. Sample matrix for categorizing business systems and applications.

Figure 3 shows an example of the result of analyzing applications and their criticality to business. This figure is only an example for selected systems and data and is intended to be illustrative not prescriptive. The actual results for any organization depend on what the available cloud-based services offer and the business's own requirements. The "telecommunications" element in the figure represents legacy non-migratable systems, although effective collaboration tools are often available in the cloud.

In addition, the figure shows how groupings can be made using the example applications listed previously. These groupings help identify potential candidates for allocation to public, private, hosted, or on-premises clouds. It is important to note that many public clouds today are more mature and secure than on-premise clouds. Often, on-premise clouds assume that the security provided by the organization's network perimeter is sufficient and therefore pay less attention to securing each application landscape, in contrast to how security is handled in a shared or external cloud. Therefore, the context of the specific organization helps determine whether the business system categories or the other factors mentioned above serve as the primary driver for the selection of the cloud hosting model.

Once the cloud-related groupings of business systems are determined, organizations should review inter-system and landscape communications, especially with respect to potential network latency impacts. Closely associated communications partners are best assigned to common locations.

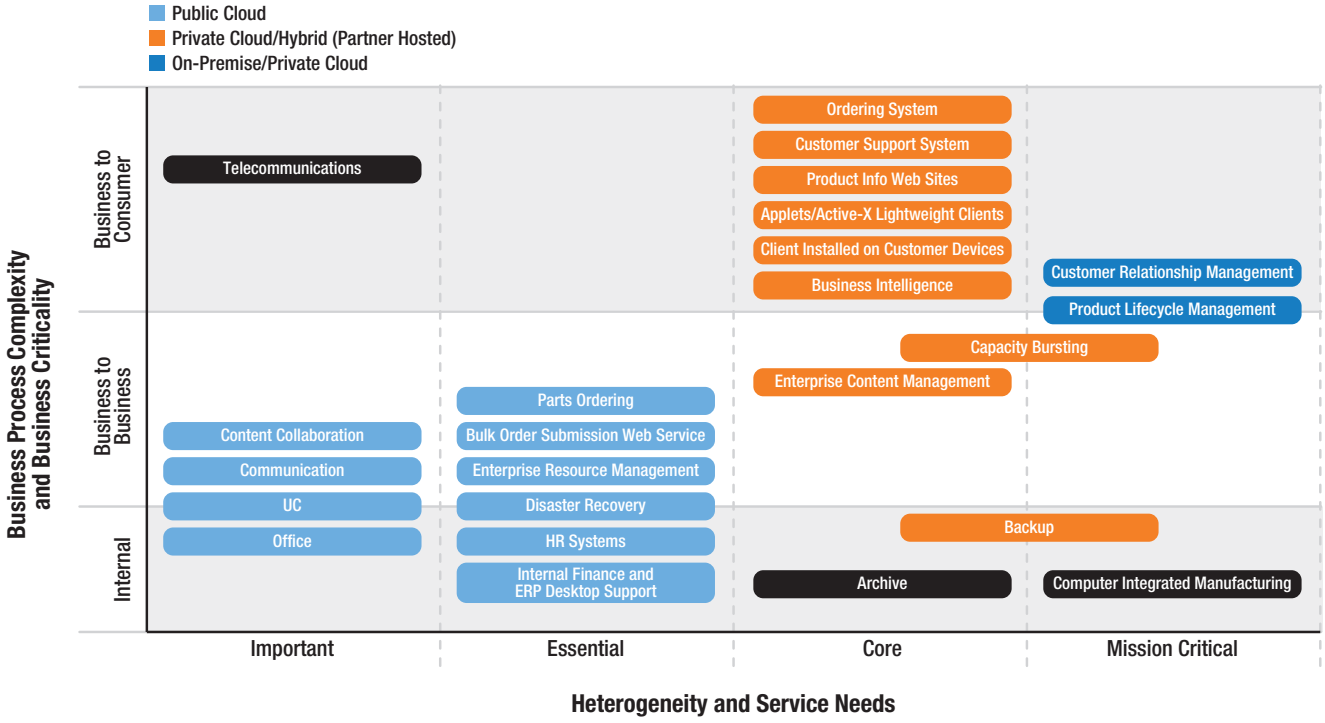

Figure 3. Example business system and application groupings resulting from using the categorization matrix.

Data Categorization

Because business data provides the underpinning for applications, it is usually considered the most important asset of a business. All systems and applications usually can be recreated quickly and relatively easily. However without the business data, they are generally meaningless. Data can include information related to the client and user, product information, transaction information, financial information, and more. Many rules that specify how data must be handled exist at the organizational, industry, country, and other levels.

A further categorization can therefore be considered for the applications above, relating to how their data should be handled and where it can be stored. Restrictions may imply the following:

- Locate within an organizational perimeter
- Locate in a secure external location
- Locate in a secure public location

And then data protection must be defined:

- Include disaster recovery
- Deploy in high-availability format
- Backup frequency (and more importantly, recovery time)
- Encryption (in transit, at rest, and on backup)
- Latency in the data chain and its potential impact on consistency

Cloud Platform Positioning

Once the cloud-related groupings of business systems have been determined (that is, critical, core, essential, or important, including data categorization), the organization should turn its attention to cloud platform positioning. It is important to position cloud-based services in the context of the entire business. That means considering both the business objectives that cloud-based services will help achieve and the organization's operational strategy.

An organization's cloud strategy should state where resources and assets will be focused and where investments will be made. The strategy should also stipulate where the organization will buy capacity, services, and infrastructure on an operational expenditure (OPEX) basis. It is also important to state how these resources will be incorporated into the business environment. Doing so helps offers maximum control of cloud-based services.

Service Models

Cloud-based services are expected to enable organizations to adopt systems and services from cloud service providers, without significant establishment costs, on a shared basis. This shared concept enables an organization to pay for only what it actually needs and uses, and to scale it in real time according to business needs. It may buy those services using one or a combination of the following two models:

- An external party provides virtual machines, and the organization deploys and operates the applications and operating systems and performs its own backups.
- The organization buys preconfigured services and systems at either the platform or software level. In this model, the organization simply performs data integration and routes system integration and transactions accordingly.

Cloud Deployment Options

Cloud deployment options[2] include infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Typically, most organizations select SaaS first for standard business processes. If an application is purchased as a commercial-off-the-shelf product, some organizations may potentially deploy that application on IaaS. For custom applications, organizations may want to consider PaaS first and then IaaS, where IaaS is typically used for custom applications that require control over the whole application stack. This type of application is usually complex and/or not cloud-aware.

Here are some further considerations about cloud deployment options:

- **IaaS.** The capability offered to the cloud subscriber is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The subscriber does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications. The subscriber may also have possibly limited control of select networking components (such as host firewalls).
- **PaaS.** The capability offered to the consumer is to deploy onto the cloud infrastructure subscriber-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.[3] The subscriber does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- **SaaS.** The capability offered to the consumer is to use the provider's applications running on a cloud infrastructure.[4] The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interface. The subscriber does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. The SaaS offering may offer the subscriber selected variables or defined options that they can customize for themselves (partially commoditized) or just offer standard application functionality which is usable but doesn't have the ability to be customized any further for any specific business (fully commoditized).

Figure 4 depicts cloud deployment options.

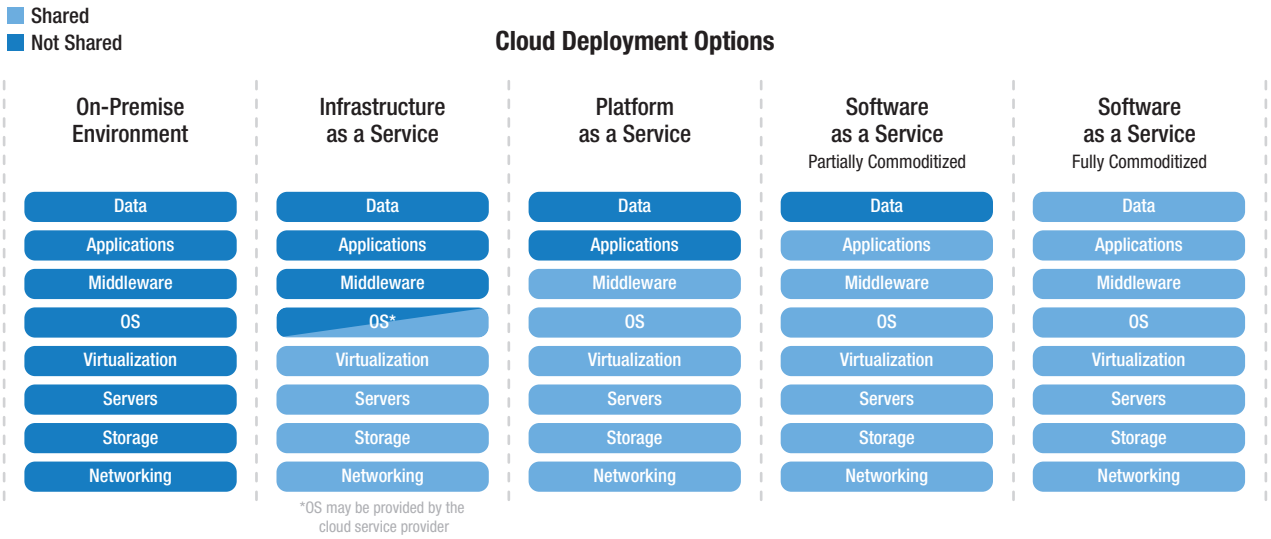

Figure 4. Cloud deployment options.

[2] Mell, P., and T. Grance, NIST Special Publication 800-145, "The NIST Definition of Cloud Computing." http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[3] This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.

[4] A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided and typically includes server, storage, and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.

BUDGETING FOR CLOUD-BASED SERVICES

As the previous section described, adopting cloud-based services requires changes to the organizational structure, and change usually requires considerable investment of time and money.

By identifying everything that must be implemented, an organization can estimate a budget that represents the total cost of ownership (TCO) for the cloud-based services initiative. In this way, the organization can track sub-area investments against the whole, as well as in context of the total benefits realized. From a financial perspective, these benefits may include cost reductions, cost savings, cost avoidance, and increased sales because of faster time to market. This budget should account for investment in people, processes, and technology. It should also include a timeline and a scope of service migration into the cloud.

This scope should address the following:

- Which services—existing or new—will be adopted
- When the services will be adopted
- Which cloud provider(s) will be used
- Cost of preparation and migration
- Potential savings that the migration will bring (such as a capital expenditure (CAPEX) reduction or removal of unused capacity)

People

IT organizations often lack the skills they need to leverage the benefits of cloud-based services. Typically, these skills include business knowledge, cloud architecture capabilities for cloud service and application design, and the ability to coordinate with groups outside of IT. Consequently, investment is required in both of the following areas:

- **Skills development.** In accordance with the IT Service Management principles under the Information Technology Infrastructure Library (ITIL), identify roles, responsibilities, and skills required for successful adoption of cloud-based services and technology, then assess these against existing skills. Identify skill gaps and develop training requirements. For IT professionals, cloud-based services represent a shift away from operational management to skills associated with service management. Such skills include identifying emerging technologies and services, leveraging these emerging technologies and services into functional solutions, setting rules, articulating the means of integration and data management necessary to protect the business, and auditing and governing compliance with these rules.
- **Operating model changes.** To make sure that the operating model reflects these new skill transitions as a result of cloud adoption.

For a more detailed discussion of skill development, refer to the Training and Skill Development section.

Processes

Cloud adoption affects all ITIL processes. However the extent of change required to reap the benefits of cloud-based services can vary and will require prioritization of processes to be changed. The following processes, which are highly impacted by cloud adoption, need to be changed first:

- **Information security.** Focus on visibility and control across an extended ecosystem, regardless of location, device, user, or hosting solution. Also include a data breach response plan as a model for cloud deployments.
- **Service continuity.** Focus on continuous availability of the extended ecosystem, such as services split across locations.
- **Configuration management.** Focus on a shift from complex and time-consuming historical approaches to image-based techniques.
- **Data lifecycle management.** Focus on data policy management, embedded workflows across engagement processes, and measurement and reporting capabilities to create and maintain data in the right places.
- **Demand management.** Focus on a shift from matching resources to demand to a focus on products or services delivered to the business from a variety of sources.
- **Portfolio management.** This is a subset of demand management achieved through a combination of project and service portfolio management, to address strategic and tactical demand.
- **Financial management.** Focus on more frequent planning cycles and more timely performance insights that meet an increasing range of requirements for compliance and control. Focus also transfers (to some degree) from a CAPEX orientation to an OPEX orientation, which potentially can have different depreciation and tax implications. Business units can drive the OPEX implication more directly than before, based on actual business requirements. These changes can make the budget forecasting a little more challenging, unless the business units themselves become part of the forecasting mechanism.

Processes that will need to be changed subsequent to those above include incident management, change management, capacity management, access management, release and deployment, service level management, and vendor management. Other processes of a lower priority can be changed as required.

The key ITIL process-related elements that should be updated to accommodate the above changes to processes include roles and responsibilities, governance, process workflow, metrics and key performance indicators (KPIs), the RACI matrix, service integration and management, and the level of automation required to support processes and monitoring.

In addition to the above processes, the enhanced processes and capabilities of cloud-based services can be leveraged in an organization's software development processes to realize significant benefits.

Technology

The path to cloud adoption requires investment in certain tools to attain the benefits as well as appropriate monitoring and control. Investment is required in the following:

- **Service orchestration and provisioning (self-service) tools.** Implement central cloud service portal for configuring and provisioning (and deprovisioning) all cloud services directly by the business.
- **Resource tracking and cost allocation tools.** Align with an upgraded procurement process.
- **Data management tool.** Include data residency; that is, tracking and reporting data compliance with corporate requirements and policies.

UNDERSTANDING COMPLIANCE AND LEGISLATION

An organization must define all of the requirements and applicability of rules that will control the handling of systems, applications, and data according to the following levels:

- Country legislation
- Industry sector requirements
- Business requirements
- Company requirements

By having these requirements defined, an auditor is able to review the deployment of classified systems and data against this set of requirements.

Sometimes it may be necessary (especially when interpretation is vague or unclear), for an organization to pre-determine the level of compliance that it wants to achieve, and the level of risk that it is willing to bear in context of the consequence, cost, or risk of non-compliance.

Regulatory compliance requires proactive focus from both the customer and the cloud service provider. In addition to business-defined requirements and obligations for providers of cloud services, regulation and standards play a key role in influencing the definition and ongoing management of cloud services. The implications include, but are not limited to, the following:

- The nature of the outsourcing contract and its terms and conditions
- The maintenance of effective business and technology controls with respect to service levels, privacy, information security, and service availability
- The maintenance of appropriate records and access provisions
- The management of service in response to business interruptions and in providing effective disaster recovery
- The ownership of data and its geolocation, taking into account privacy, cross border, and availability-based regulations and mandates
- Privacy; information security; intellectual property
- Data ownership and cross-border data flow; data residency and location
- Breach management
- Service levels, business continuity, availability, and disaster recovery
- Commercial and contract law; dispute resolution
- Forensics, eDiscovery, logging and auditing, and data return
- Tenancy, software exports, and encryption strength

Additionally, a cloud strategy may require the organization to proactively communicate with the regulator or regulators that impact the organization and its jurisdiction. The organization must also manage potential reputational risks, regulatory compliance risks, and risks relating to maintaining transparent relationship with the regulator.

We recommend that cloud subscribers also develop an ongoing corporate compliance and risk management program for periodic review of regulatory requirements and changes, industry standards, internal processes, and cloud provider operations, including audit and compliance. A corporate compliance program would therefore include processes for the following activities:

- Monitoring laws, regulations, and standards
- Performing impact analysis of compliance obligations resulting from regulations, laws, and standards
- Updating risk and compliance frameworks
- Implementing controls to manage compliance risk
- Monitoring, auditing, and reporting on compliance posture
- Taking corrective action as required

DETERMINING PREREQUISITES AND KEY ENABLERS FOR CLOUD ADOPTION

To effectively take advantage of cloud-based services and integrate them into an organization's technical environment, a number of enablers make sustainability and benefit recognition much easier. Cloud enablers allow an organization to build, deploy, integrate, and deliver cloud computing solutions.

ODCA Cloud Maturity Capabilities

The ODCA Cloud Maturity Model maps cloud maturity from two key perspectives: business capabilities and technology capabilities.

- **Business capability.** Offers a comprehensive view of the maturity model's stages through the lens of "business use of the cloud." This perspective includes a mix of cloud service models, cloud deployment models, and cloud capabilities across four business categories: business strategy, organization and skills, projects, portfolio and services, and governance.
- **Technology capability.** Provides a similar comprehensive view of an organization's cloud maturity, but does so through the lens of cloud technology across four categories: operations, administration and governance, information, infrastructure, and architecture.

For more information, see the ODCA Usage Model: Cloud Maturity Model Rev 2.0.[5]

Key Enablers

Cloud computing offers the potential to respond more effectively and dynamically to technology trends that are rapidly reshaping how enterprises operate (examples of such technology include mobile technology, data analytics, and social media). It is a potential game changer, with the power to shift competitive landscapes by providing enterprise-level technology and scale to new business initiatives, allowing more nimble operations, faster time to market, and an ability to scale.

However, cloud computing differs significantly from traditional forms of outsourcing. To effectively take advantage of cloud-based services and integrate them into an organization's technical environment, a number of enablers make sustainability and benefit recognition much easier. Cloud enablers allow an organization to build, deploy, integrate, and deliver cloud computing solutions. Figure 5 depicts the key enablers required for effective cloud adoption.

[5] www.opendatacenteralliance.org/library

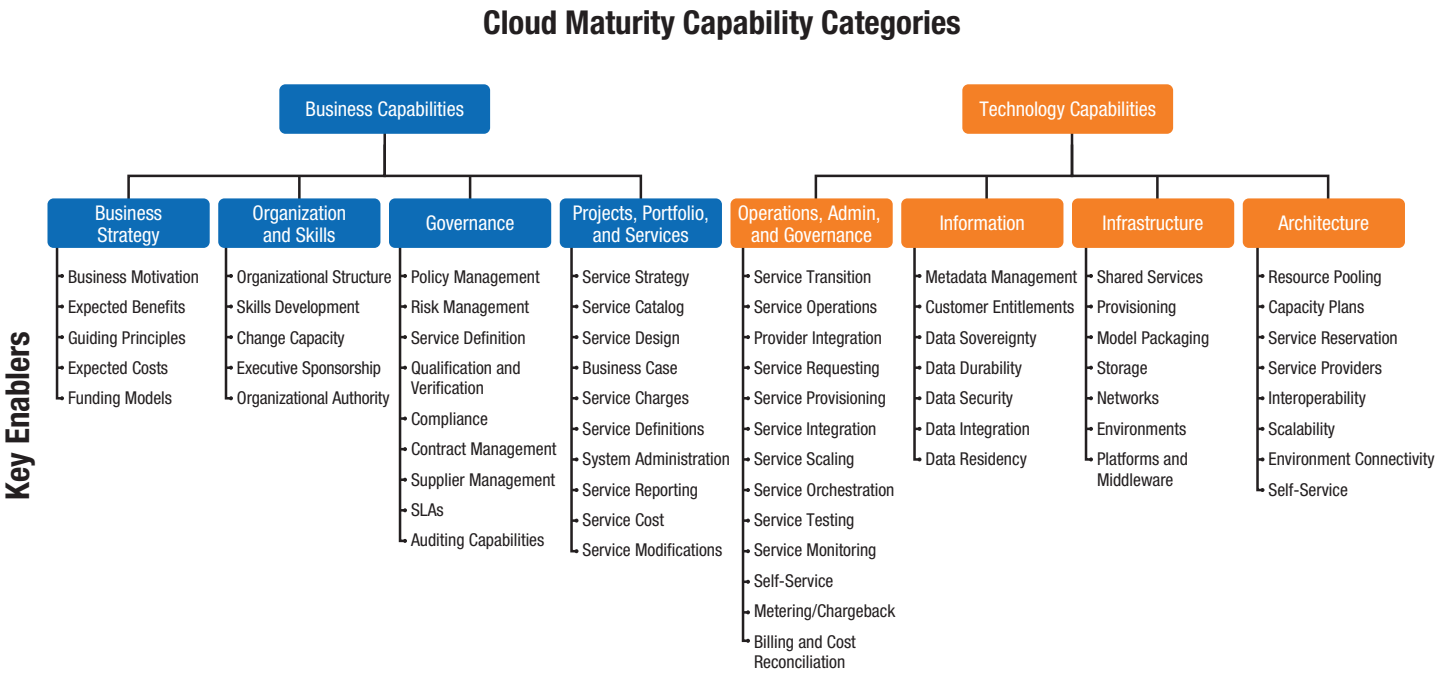

Figure 5. The key enablers required for effective cloud adoption.

These key enablers can be considered from two perspectives: the business capabilities perspective and the technology capabilities perspective. Each of these is described in the following two sections.

Business Capabilities Perspective

From the business capabilities perspective, key enablers for cloud-based services adoption can be categorized as relating to the following areas:

- **Business strategy.** Strategic enablers that guide the cloud strategy.
- **Organizational considerations.** Enablers at the organizational level, such as skillsets and change capacity.
- **Governance.** Enablers associated with the governance structures and processes that support and guide the cloud efforts. The maturity and adoption of adequate governance is a leading indicator of the overall success of a cloud computing strategy.
- **Projects, portfolios, and services.** Enablers that relate to the planning and building of cloud-based services, and the management of the portfolio of services.

Tables 7 through 10 provide additional details on each enabler.

Table 7. Business strategy enablers.

Enabler	Description
Business Motivation	Specifically define what services can and cannot move to the cloud
Expected Benefits	Financial and non-financial benefits, such as cost reduction and simpler, more reliable service offerings
Guiding Principles	Any rules that relate to core services or data sensitivity
Expected Costs	Based on both cloud service provider and internal process and orchestration costs
Funding Models	Pay-for-use, regular subscription, block scale units, and so on

Table 8. Organizational enablers.

Enabler	Description
Organizational Structure	Areas of responsibility for managing cloud components and role of each area
Skills Development	Existing skills, skill gaps, and training requirements
Change Capacity	Takes into account other projects that may be happening across the organization
Executive Sponsorship	Identify the individual executive driving this initiative
Organizational Authority	Identify who can approve various levels of requests

Table 9. Governance enablers.

Enabler	Description
Policy Management	Identify who owns the policies and how and when they are revised
Risk Management	Understand and be capable of monitoring the risks associated with cloud adoption
Service Definition	Define what a service is, including scope, objectives, outcome, accountability, roles, inputs and outputs, and assistance in identifying service candidates
Qualification and Verification	A short list of pre-qualified providers to streamline the addition of services, and a process for qualifying new providers
Compliance	Process to help providers and users comply with the conditions set for cloud usage
Contract Management	Legal review of contracts, plus planned reviews and contract renewal
Supplier Management	Planning and execution of interactions with providers and suppliers in a coordinated fashion across the organization, including selection criteria
Service-Level Agreements (SLAs)	Performance standards for services provided and requests for additional services
Auditing Capabilities	Audit processes and reporting to assess and assure compliance

Table 10. Projects, portfolios, and services enablers.

Enabler	Description
Service Strategy	Specify the key services for the business, including any services being discontinued
Service Catalog and Service Portfolio Management	Current services defined centrally, plus what services are in the pipeline, especially those that may impact existing services
Service Design	Includes service continuity, capacity management, security management, configuration management, and license management
Business Case	For each service being considered for transition or transformation
Service Selection	Includes criteria, timing, and dependencies
Service Charges	Pricing, including service packaging and peak time rates
Service Definitions (Service Composition)	Includes service identifier (for common communication between parties), service processes and workflows, service hours and expected capacity, operations support required, roles and responsibilities, monitoring and tracking requirements, processing and data restrictions (for example, not off-shore), data validation and retention, service-level required including acceptable turnaround times, performance measures, continuity times, restoration or remediation, escalations and monitoring, service request options and costing, post-deployment tasks and automation scripts, service and deployment dependencies, notification methods for service events and alarms, and service administration
System Administration	Subscriber ability to administer access and authority to the provider's service catalog, including remediation
Service Reporting	Accessibility of data to make sure all required reporting can be delivered, such as regulatory reports and key performance indicators
Service Cost	Understand the current costs of service provision to get a true sense of value and benefits
Service Modification	Define triggers for service modification: performance, business requests, and capacity thresholds

Technology Capabilities Perspective

From the technology capabilities perspective, key enablers for cloud-based services adoption can be categorized as relating to the following areas:

- **Operations, administration, and governance.** Enablers related to the post-deployment aspects of cloud-based services: the operations, administration, and management aspects of the cloud environment.
- **Information.** Enablers associated with the data and metadata aspects of cloud-based services.
- **Infrastructure.** Enablers associated with the service infrastructure and tools that provide the technical foundation for the cloud initiative.
- **Architecture.** Enablers related to the definitions of overall architectures and guidelines for various cloud service architects and application development practitioners to promote adherence to the desired cloud best-practice architecture.

Tables 11 through 14 provide more details.

Table 11. Operations, administration, and governance enablers.

Enabler	Description
Service Transition	Release and deployment management and change management
Service Operations	Request fulfillment, incident management, and security
Provider Integration	Specify how the cloud service provider will be involved in resolving incidents and problems, and implementing change
Service Requesting	Includes new services, capacity changes, modifications to existing services, suspension/resumption of services, altering dependencies, request construction, verification that the cloud service provider has made available the resources requested, authorization and release, and service deletion or capacity reduction (ensuring that this results in the resources being returned to the cloud pool and charges are stopped)
Service Provisioning	Includes access authorization/authentication, request authorization hierarchy (who has permission to request what services), and Internet access to services and a service request graphical user interface (GUI). Details should include whether the GUI is available from mobile devices, usage monitoring and reporting, and auditing (including activities outside of normal hours)
Service Integration	Existing services that the new service relies on or will impact
Service Scaling	Address scale-up and scale-down and the lead-times for these to take effect
Service Orchestration	Ability to orchestrate multiple services, service components, and providers
Service Testing	Testing capability including disaster recovery and continuity
Service Monitoring	Performance monitoring and comparison to service-level agreements
Metering and Chargeback	Ability to measure and report on usage, and chargeback to internal divisions for cost recovery
Billing and Cost Reconciliation	Process to verify charges and escalate discrepancies. This must take into account services from multiple providers.
Self Service	A list of functions users can request without higher authorization

Table 12. Information enablers.

Enabler	Description
Metadata Management	Defines the information and service data and how it is maintained
Customer Entitlements	Down-selected functionality from the total potential service catalog, available to business consumers based on their roles and responsibilities
Data Management and Ownership	Includes ownership, access, encryption, masking, retrieval, recovery (normal or termination of contract), transition to another provider, backup copies of data, handling of test data, and archiving and deletion verification
Data Durability	Data integrity and recoverability when data moves between devices
Data Security Policy	Data sensitivity and classification
Data Integration and Synchronization	How data will transverse, integrate, and synchronize with systems and services while maintaining its integrity
Data Residency	Where data resides including any restrictions (for example, off-shore may not be permitted)

Table 13. Infrastructure enablers.

Enabler	Description
Shared Services	Defines assets that are shared between services or between subscribers
Provisioning	How assets will be made available. Includes notification and verification.
Model Packaging	Template/pattern combinations of assets for better pricing
Storage	Capacity and reliability
Networks	Access, security, lag times, and capacity
Environments	Production, testing, development, and so on
Platforms and Middleware	The types of assets, including operating systems, emailing, and databases

Table 14. Architecture enablers.

Enabler	Description
Resource Pooling	Total pool from which all services can draw upon for their resources
Capacity Plans	Both current and planned service, to foster negotiation in advance for the best provision
Service Reservation	Includes minimum capability and capacity levels, reservation for specific services, blocks of increases (for example, if 80-percent capacity is reached, automatically initiate another two servers of capacity x; if less than 20-percent capacity, automatically decommission servers down to the minimum reserve). Include definition of block scale units.
Service Provider(s)	Required for certain elements of the service
Interoperability	The extent to which systems and devices can exchange data and interpret that shared data
Scalability	The ability of a system, network, or process to handle a growing amount of work in a capable manner
Environment Connectivity	The ability to run a service or application on many connected devices at the same time
Self Service	Resource alteration requests

Guidance and Recommendations

All of the above enablers need to be considered for each type of cloud deployment model (IaaS, PaaS, SaaS, and Information-aaS) and for all hosting models—public, private, hybrid, and other evolving cloud delivery models (such as XaaS).

As a recommended check, a cloud subscriber can engage a registered CMM Assessment agent and give an assessment of the subscriber readiness and alignment to the above enablers. This assessment should include suggestions of areas for improvement and preparation. The cloud subscriber can also conduct the testing scenarios as laid out in the ODCA Master Usage Model: Service Orchestration document.[6] This will assist with verification of the subscriber and providers involved and the services selected for cloud provisioning.

[6] www.opendatacenteralliance.org/library

MAKING THE NECESSARY OPERATING MODEL CHANGES TO SUPPORT CLOUD STRATEGY IMPLEMENTATION

Cloud adoption is more than mere technology. To realize the maximum benefit from cloud adoption, organizations must implement many changes throughout the organization. These include changes to organizational structure and culture, providing adequate training to build the necessary skillsets, maintaining control over procurement of services, and aiding business units (and sometimes external partners) as the cloud adoption initiative progresses. Each of these areas is discussed in the following sections.

Organizational Structure

Because cloud-based services are a relatively new concept, most business are still structured to use in-house or directly outsourced IT services. Typically the organizational structures and capabilities to manage and maintain those structures and services are geared to some level of direct control and involvement. In this model, the in-house IT organization is usually in direct control, positioned between business units and IT. Business units must request services from IT, and a procurement process may then follow, with provisioning and setup projects in line before production and operational readiness. The organization is represented in this chain through a well-controlled linear progression of a request, over some time, through various teams, each applying their skills and capabilities. The request then returns through the same path indicating final delivery of the service.

Cloud-based services begin to drive the need for change. Services can be bought by anyone in an organization, online, and potentially accessed over the Internet. This raises the concern of potentially bypassing all governance and controls, procurement, IT, and risk management processes, with the services being operated outside of the auditing perimeters; that is, until a problem arises.

Rather than place more controls and inhibitors to prevent such occurrences, organizations can direct their focus to creating a structure that fosters fast, intuitive, and controlled use of cloud-based services and technology. Existing organizational control models should be updated to be cloud-centric. These control models should be able to effectively support structured use of selected predefined cloud-based services, for specific purposes, with self-service and automation, within a defined framework of policies, procedures, and standards, all of which are aligned to business objectives.

Key Areas for Organizational Changes

The key areas to consider where structural changes could be advantageous include:

- Core business units of the organization
- Service delivery management
- Procurement
- Risk management
- Security (including information security)
- Internal audit
- Finance
- IT services
- Project management and delivery

The Service Delivery Management group, which may be new, manages the required contracts, operational-level agreements, and service-level agreements (SLAs) for cloud-based services. This group also administers the commercial aspects of cloud-based services and performs planning and incident communication and prioritization. Further details about this organization's roles and responsibilities are described in the Governance and Controls section.

Typical changes to the overall organization may include those shown in Table 15.

Table 15. Typical organizational changes required to support cloud-based services.

Team	Current	Future
Business Units	• Randomly explore any available cloud service to meet their requirements.	• Learn how to interpret requirements, categorize systems and data, and interpret services for selection and compilation from a cloud service catalog.
Service Management	• Focus on studying reactive reports from suppliers and negotiating improvements.	• Become an integrated and active group between cloud subscriber and cloud provider, in real time, to drive proactive service outcomes.
Procurement	• Generate request for proposals for services, solutions, and items. • Select from available offerings. • Procure services and track delivery.	• Move to online service procurement portal and processes, processing, and delivering services in real time.
Risk Management	• Define categories, define written rules per category, and monitor achievement and risks.	• Move to defining online rules in real time and integration of risk policy logic and requirements into service orchestration engines, and observing landscape reports for compliance, potentially in real time.
Internal Audit	• Review controls within systems and services against risk and compliance requirements of the organization.	• Updated measurement and reporting criteria, including use of assets and services located in other legal and physical jurisdictions, often shared between dissimilar industries.
Finance	• Restrict investments and operational costs to planned budgets.	• Set the framework for service consumption within metered limits. • Receive invoices from various providers (based on authorization previously issued for service procurement).
Information Technology Services	• Define rules for use of "their" services and assets, and deliver structured planned services to the business (either in-house or outsourced).	• Become a consultant to the business, addressing cloud readiness, preparations, and education. • Participate in integration and control work between various service elements. • Manage global policies for security, cost, and workload placement.
Project Organization	• Coordinate between various teams and specific deliverables.	• Facilitate requirements definition and service selection in terms of business objectives, with real-time resource coordination and much faster delivery timelines.

The Transformation of the IT Organization

As an organization begins the transition to cloud-based services, the positioning of a part of the corporate IT organization begins to change (see Table 2). A part of the organization definitely remains in place, to manage certain systems, networks, and capabilities. However, the part of the IT organization that supports the systems that migrate to the cloud needs to be repositioned. If the IT organization itself establishes and provides a private cloud service, then IT needs to transition to the role of a service provider of an outsourced service, including legal, technical, commercial, and service-level capabilities. The IT team members that move into the facilitation role on behalf of the organization, somewhat similar to a "broker," must develop a strong service management capability. This brokering group will begin acting as the go-between in the service chain from the business units (cloud subscriber) to various cloud providers and partners. As shown in Figure 6, the brokering group will translate needs and services, help select services, and overlay rules, policies, and governance onto the services and requirements on behalf of the business units.

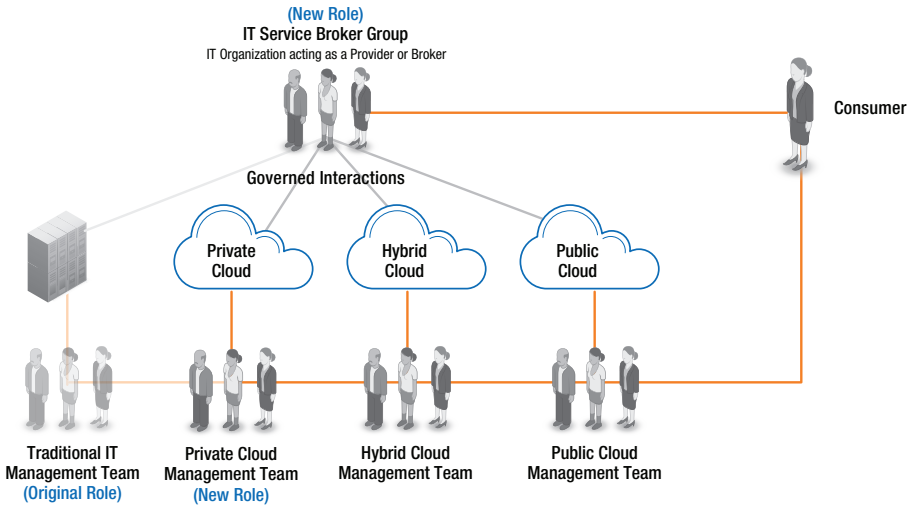

Figure 6. How cloud-based services transform the role of IT.

Organizational Culture

In the context of cloud computing, IT is built, run, and consumed differently. IT is also governed differently. To effectively adopt and sustain cloud computing for the benefit of the organization, a right-sized structure and culture is required to deal with divestment of choice and control of provisioned IT services. There will be a significant amount of healthy tension and competition between internal IT services and services offered by cloud service providers. A cultural shift will help the organization support the business with choice, innovation, and flexibility, as well as manage the transformation that is required from the IT organization. Some of the aspects of this cultural shift include the following:

- **Competition.** To remain viable in the IT services free market, corporate IT needs to compete with cloud service providers by being more responsive, transparent, and relevant to business users.
- **Brokering.** Corporate IT should transform from being a gatekeeper of information, to a free market broker and orchestrator of IT services. The operating model should shift from a traditional plan, build, and run model to a model that supports conceptualization, assessment, selection, orchestration, and governance of IT services. A culture of specializing in IT governance related to cloud-based services is essential.
- **Role in the ecosystem.** Corporate IT should transform from being a supplier to being a business partner. The goal is to increase the transparency of the consumption model by communicating effectively with the business stakeholders, and to promote the relationship between demand and supply, consumption, and cost. This approach will increase financial transparency of IT costs.
- **New mandates.** Corporate IT should redefine its focus from being a provider of standalone components and custom infrastructure for each project to being a provider of an integrated, tested, and ready-to-grow infrastructure. This is achieved by the following means:
  - Create a standardized set of enterprise-class services based on business needs, as opposed to customization
  - Loosen business units' attachment to named servers, devices, and configurations, and redirect them to scalable cloud-aware and cloud-based services
  - Develop the capability for elasticity, data center growth, and movement of workloads and data between internal and external data centers
- **Innovation and agility.** Corporate IT must increase employee productivity through innovative applications and a culture that nurtures innovative practices through self-service and automation. This can be achieved by delivering a self-service catalog with standard offerings to accelerate business unit experimentation and innovation.
- **Elimination of silos.** Shifting from a silos mindset to a services mindset is required. IT employees need to align their efforts with services that the business units find valuable. Business transformation requires business leaders with vision to break down organizational and information silos and transform the entire corporate culture. This requires that IT engage with business users in a proactive, outward-focused approach rather than a reactive, infrastructure-focused fashion.
- **Efficiency and accountability.** IT should help business units increase efficiencies and lower operational costs through increasing IT efficiency and reducing operational costs. In addition, IT should guide the business on security, privacy, and regulatory best practices.
- **Service orientation.** An organization should develop new competencies and capabilities for service management and delivery, including areas such as demand management and capacity planning. IT should create an initial standard service catalog, along with the processes, tools, and training required for effective product management across the services portfolio.

Training and Skill Development

The ODCA believes that elevating IT skills to meet the rising demand for applications that take full advantage of cloud capabilities requires ongoing education and training of the existing workforce. Nurturing internal talent and preparing the developer workforce to architect cloud-aware services is a smart investment. It is also an effective way to protect the domain knowledge that IT has built. Over the years, dependencies on key IT personnel become critical, particularly those individuals who have developed subject matter expertise and business domain knowledge of the organization. This organizational knowledge is hard to replace—it takes many years to train new incumbents to reach a level of expertise about the business domain of an enterprise. Enlightened organizations can benefit from identifying the best ways to retain knowledge within the fabric of the organization.

As discussed earlier, cloud adoption requires new skills for the IT organization, similar to those necessary when an organization decides to outsource. In both cases, after transferring many responsibilities to the outsourcer or the cloud service provider, the internal IT organization slowly rebuilds itself and begins to compete with the outsourcer or provider.

In the case of cloud adoption, the internal IT organization often has strong competencies in the infrastructure, which now becomes the most basic internal role of the cloud service provider. This situation leaves the original IT group without a base foundation and with limited transparency and control of what is built and how. In response, the IT group must refocus on connecting to and integrating the provided cloud services. These services can include infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). (For more information, see the Cloud Platform Positioning section.)

The IT group must maximize for the business the opportunities and features that the cloud service provider offers. If the internal IT organization is the cloud provider themselves, they have to standardized elements and teach the business units how to effectively prepare for and use their services. The enterprise private cloud must provide a positive user experience with easy-to-use tools and automation including APIs at every layer. IT must also learn about service provision concepts and frameworks, because they are in effect replicating and competing with the public cloud. IT must also learn about unitized charging (chargeback and showback), cost transparency, cost effectiveness, and competitive advantage.

Skills and training are also important for non-IT organizations, such as procurement, business users, risk and compliance staff, and Information security. The following skills will foster cloud-based services that lead to business transformation:

- **Effective virtualization.** In the context of the private cloud, an understanding of IT assets and environment and a strategic intent to simplify, consolidate, and standardize virtualized services.
- **Converged technology architecture roadmap.** Able to develop such a roadmap, commit investment, and sustain the business buy-in necessary for business transformation.
- **Cloud-aware applications.** Develop applications that take advantage of new architectural patterns and changes in the way applications are designed. There is a misconception that architecting an application for the cloud is just like architecting an application for a virtualized environment. To take advantage of the unique capabilities of the cloud, developers must adopt an application architecture that's designed for the cloud. Program applications to be aware of the distributed infrastructure on which they now reside, resulting in better redundancy and performance.
- **Integration.** Able to bridge or integrate data between disparate systems, based on both the enterprise and public clouds.
- **Communication and organizational change management.** Communicate cloud initiatives across the entire organization. The success of any new application and cloud strategy depends on strong communications skills to successfully manage the transition.
- **Operational strategies.** Develop operational strategies that support deployment and operation of applications in the cloud. IT skills are required to offer redundancy, utilize caching, stage deployments, plan for zone or region failures, minimize inter-zone latency, and manage IT operations across several cloud service providers.
- **DevOps (Development/Operations).** Merge development and operations to accelerate innovation and agility and sustain business transformation through continuous delivery cycles.
- **Sourcing and commercial acumen.** Carefully negotiate and continually monitor cloud-based service contracts. This requires an increased focus on sourcing and commercial management skills.
- **Risk assessment.** Translate technology risk to business risk in a way that doesn't alienate business units, and persuasively present information security as an enhancement rather than a hindrance.

Shadow IT Prevention

Shadow IT is hardware or software within an enterprise that the organization's central IT department does not support. In the past, shadow IT was often the result of an impatient employee's desire for immediate access to hardware, software, or a specific web service, resulting in procuring the resource without going through the approved channels. With the consumerization of IT and cloud computing, the meaning of shadow IT has expanded to include personal technology that employees use at work or niche technology that meets the unique needs of a particular business unit and is supported by a third-party service provider or in-house group, instead of by corporate IT. This new context includes the use of SaaS and the use of IaaS for data backups or disaster recovery purposes.

IT needs to provide self-service interfaces and make it easy for business units to use IT—avoiding manual service requests. By doing so, IT avoids the problem of business units engaging directly with cloud providers, which has the following disadvantages:

- Business pays for multiple instances of a single provider's application (application sprawl)
- Potentially higher costs per instance, due to the inability to negotiate pricing based on a larger customer base

The organization can address the problems of shadow IT evolution through a combination of prevention, detection, and response to the discovery of shadow IT.

Prevention

Educating the business stakeholders on the inherent need and benefits of procuring and managing IT through the organization's proper channels and IT department is a significant mitigation plan to preventing shadow IT. A good first step typically is to create a transparent and focused understanding of the risks of shadow IT and the benefits of procuring IT through the IT organization.

This strategy needs to be enriched with organizational policies and standards to clearly spell out the enterprise mandates for preventing shadow IT. The appropriate governance and approval mechanisms for IT expenditures must be in place. Relationship managers or service owners accountable for specific cloud services within an enterprise can play a strong role in preventing cloud sprawl, through control mechanisms and governance of services.

Detection

Detecting shadow IT through procurement audits, expense reports, review of credit card activity, and payment transactions could be effective in understanding where cloud services have been procured without enterprise governance. Requests for message specifications or data formats can also be a telltale sign that someone in the enterprise is attempting to integrate the organization's internal systems with cloud services.

Security, network, and bandwidth usage monitoring can also be used to detect shadow IT.

Response

Organizations can apply consequence management practices to deal with instances of shadow IT and unauthorized procurement of cloud services (although this is a response technique after shadow IT has been discovered). If unauthorized cloud services have led to intellectual property (IP) violations or could cause security exposures, appropriate data protection and IP protection response plans should be enabled. The root cause of shadow IT should be investigated and steps taken to prevent further occurrences through governance and remediation plans.

Taking Business Partners on the Journey

Commencing a journey with an organization means that one is taking an ecosystem down a particular path of exploration toward new frontiers. Both internal and external partners must be considered:

- **Internal business units.** These are business unit or business unit functions such as marketing, sales, manufacturing, planning, human resources, and finance.
- **External suppliers.** These are separate legal entities but are usually directly in the organization's product path and value chain from creation through the end client using a product of the organization. External suppliers can include suppliers of materials and financial partners such as banks, dealerships, and agencies—anyone who may share data or systems with the organization or interact at a system level.

Each business partner must be handled appropriately, but some important things organizations should address for both groups include the following:

- Communicate about the cloud intent, the adoption plan, the timeline, and the expected changes associated with adopting cloud-based services.
- Focus on "what's in it for them." Answer that question from their perspective as thoroughly as possible, but allow them room to explore, too.
- Prepare partners for the realization that they may lose some revenue to or from you and may potentially experience other impacts and costs, but they can also gain benefits.
- Make it easy. Create guides, blueprints, and checklists, and include these in the project planning as appropriate.
- Take the fear out of the cloud adoption process by sharing examples of success and using known and trusted references.
- Avoid making a power-selling sales pitch. Instead share the concept, then listen, listen, listen, and agree upon actions, risks, and mitigations.
- Don't "cloudwash" everything. Cloud works for some things and not for others—be realistic and practical.
- Share learnings.
- Review contracts and update them as needed.
- Be clear about the roles and responsibilities of the business partners in the context of the cloud model. Also create the understanding about the "services" model that is inherent in cloud computing and how service-level definition, management, and governance would play an increased role in the relationships between the organization and partners.

ROLLING OUT THE STRATEGY

The previous sections have discussed the many decisions an organization must make as it builds a cloud strategy founded securely on business goals and objectives. With the strategy clearly defined, implementation involves setting a timeline for milestones, communicating the strategy across the organization to maximize the strategy's effectiveness, and choosing an appropriate cloud adoption model. The following sections address each of these topics.

Timeline

Nothing happens overnight in a large organization. In the context of cloud service adoption, how long it takes the organization to implement its cloud strategy involves a number of considerations. Assuming that the adoption of cloud services will be a key enabler in the business transformation agenda of the organization, one must consider two key areas:

- **Initial adoption of cloud services.** This relates to the time from start of a formal cloud initiative to having business systems in production on cloud services and expected benefits that begin to result.
- **Cloud benefits realization.** This relates to achieving the maximum potential benefit of cloud services.

Simply migrating business systems toward cloud-based services may initially result in limited organizational benefits. The level of maturity (in the context of the ODCA Cloud Maturity Model) significantly affects an organization's ability to achieve maximum potential benefit from cloud-based services. Moving from one maturity level to the next, and eventually reaching the most mature level, may take additional time to achieve.

This means that as the organization increases the maturity level of its cloud-based services, thereby increasing capabilities, the degree of benefit realization should also increase. For example, moving from a manual (people-driven) scaling of systems based on cloud platforms (at approximately CMM Level 1), toward automated scaling with federation of system components distributed between the most appropriate platforms for each system element (approximately CMM Level 4+), will result in significantly more benefits with respect to speed of capacity allocation, quality of service, efficiency of changes, and costs for the business.

The longer it takes an organization to adopt cloud-based services and achieve the target cloud maturity level, the more the organization potentially supports duplicate cost structures, with limited benefits materializing during that time. It is therefore beneficial (in the context of the organization's business requirements), to set a realistic time frame for when the benefits realization should occur. This time frame should be aligned to the business transformation agenda.

Communication Plan

Cloud-based services as a new business enabler are important to the organization. The adoption of these services may lead to the following:

- Enable selected business objectives to be achieved
- Drive change in certain work functions and processes
- Change the risk landscape of the organization
- Change the investment strategy of the business with regard to operational and capital expenditures
- Require the establishment of new skills

Therefore, it is important to communicate the business value of cloud-based services to the entire organization, both IT and business units. This communication should include what the cloud strategy involves and why it has been implemented. Absence of communication may lead to confusion and frustration, with resulting conflicts. It may also cause individual areas to exploit the resulting opportunities to deviate from accepted standards, in the absence of clear guidelines. Figure 7 represents a possible model for this communication plan.

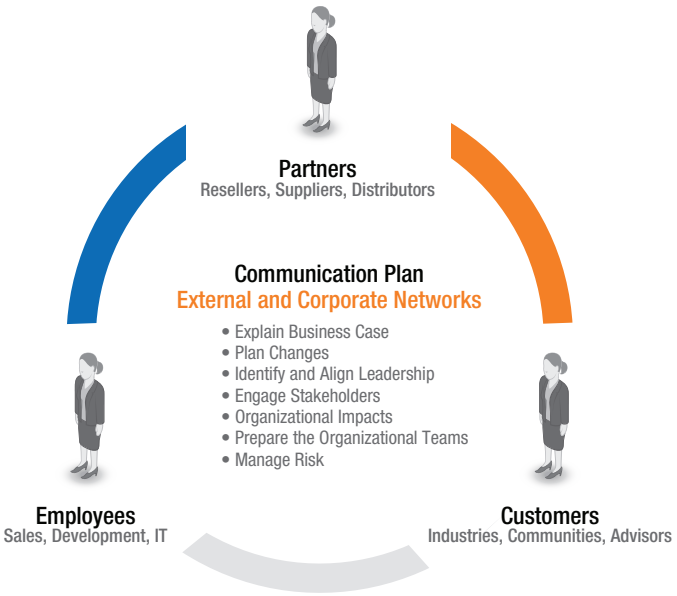

Figure 7. Plan for communicating the cloud strategy across the organization.

Each business unit and stakeholder should be given a clear understanding of the cloud strategy, in the context of their business objectives and goals, including appropriate dimensions. This communication should be provided in a way that is practical and referencable (that is, easy to find, easy to use) by all business units, serving as a guideline to decision making; the strategy should not just be an addition to the corporate shelf-ware; it should be usable daily as a guide in making choices and decisions.

It is well known that communicating an idea only once does not result in successful change management. In fact, organizational understanding generally matures only after 7 to 12 communication events, depending on the complexity of the concept being communicated. These repeated communications should usually not simply duplicate the original communication, but should restructure it from various angles, to make sure that the concept is thoroughly understood.

Sub-organizations or teams may want to apply the strategy differently, or understand it differently, especially if they cover different scopes. For example, marketing will have different needs than production. Potential impacts to discuss at individual communication sessions include the following:

- Human resource, financial, and service impacts
- Goals and objective opportunities
- Issues and concerns

Table 16, on the next page, provides some guidelines for communicating an organization's cloud strategy.

Communication requires time and resources, but the guidelines provided in Table 16 should result in a well-aligned business, with better support for governance and controls, and improved future return on investment.

Organizations should define measures for these communication activities and track concerns and issues. For example, if labor unions or workers councils are active, they must agree to the preparations and potential job changes of individuals, and their support must be solicited.

The communication plan should be planned with the internal human resource and training organizations, and then incorporated as part of the projects for implementation, starting at budget time and working granularly from there. It is important to position the cloud strategy as a positive leap into the future, ensuring competitiveness in the market and improved capability for the achievement of business objectives, and thereby the sustainability of the company. Also emphasize in a positive manner that the employees of the company are being taken along on this journey and moving forward with new skills development, new opportunities, and new capabilities.

In parallel, a section in the regular corporate communication medium should be introduced to report and track the cloud-based service progress, and possibly to introduce an important cloud concept in each issue. This will ensure that the cloud initiative becomes well known and familiar to everyone over time, instead of being seen as a threat or something to ignore or circumnavigate.

Table 16. Guidelines for communicating a cloud strategy.

Communication Type	Goal	Content
High-level, company-wide, leveraging different channels: direct email, social media, and a hosting service catalog	Position the adoption of cloud-based services and the cloud strategy. Show how cloud-based services relate to business objectives and describe the expected benefits. State that team-orientated interactions will occur, customized to each team, addressing important considerations.	High-level timeline Description of key enablers that include the following: • Policies (including corporate compliance and legal dimensions) • Rules • Guidelines • Systems • Contractual agreements
Focused communication targeted to each affected business unit (assigning representatives and serving as a channel to gather requirements)	Define a future view and agree on an action plan.	• Relative business goals, the teams' contribution to them, and potential positioning of cloud systems in that context • Potential opportunities, risks, threats, and strengths in context of the team • Training and further changes or interactions that are planned • Important processes and considerations that the team should be aware of, in the context of cloud-based services
Repeat communications to business units	Underscore the main message and provide further information.	• Scheduled work sessions for Q&A, planning, and impact interpretation
Pre-written communication with any involved regulators and the media	Define the scope of the cloud strategy.	• Initial timeline • How changes will be managed • What benefits the business intends to gain from cloud-based services • How potential new risks are being identified, assessed, and addressed • Comments on the importance of the reputation of the business and how (in the context of cloud computing) that reputation will be maintained and enhanced, such as faster product development or cost reductions
Communication with the organization's partners	Include these important stakeholders in the overall cloud strategy implementation.	• Ask for inputs and recommendations • Delineate areas where they can support or participate in the strategy • Potential impacts to them • Changes they should prepare for (such as service scopes, contractual agreements, exclusivity clauses, skills development, and potential revenue changes)
Build the strategy into processes and tooling	Make it easy for end users to consume and apply the strategy.	• Create self-service portals, catalogs, and other automated tooling • Create short, self-service videos to reinforce key concepts • Create channels for feedback using tools such as social media

Cloud Adoption Models and Consequences

To make cloud service adoption and migration a repeatable and predictable process, we recommend the use of cloud-based service blueprints. These blueprints will create a proven framework for all project teams to leverage. Of course, during subsequent projects, teams can make improvements to this framework. But having a known (and eventually trusted) reference framework gives all teams that follow the initial proof of concept and first application migration both proof and confidence that their potential risks are minimized. The reference framework also makes the migration "hurdle" more achievable and less of a threat.

There are a number of different potential approaches to cloud-based service adoption, and each of them triggers different responses and results from the organization. Each company must determine the best approach, based on current maturity, entrenchment of current work practices, and other considerations. The sections below list a number of these models, considerations, and impacts, from two perspectives:

- Exactly what cloud-based services can move to the cloud
- How cloud-based services can move to the cloud

The "What"

Table 17 describes what cloud-based services can be adopted in an organization. It provides alternative blueprints for deciding the principles that drive "what" can be cloud-centric or cloud-enabled. Each model has advantages and challenges, and different business units may adopt one or another model, depending on their specific business needs.

Table 17. Models for deciding what cloud-based services can be adopted.

Model	Description	Advantages	Challenges	Outcomes
Growing the Cloud Inside Out	Many internal cloud computing initiatives, supported by internal virtualized cloud computing environments (an internal private cloud). Suitable for a technology savvy enterprise and is an important enabler where legacy systems and environments need to be maintained for extended periods of time.	• Delivers economies of scale. • Protects security exposure in industries that are extremely sensitive to intellectual property protection. • Provides large-scale learning opportunities for the organization's IT and business workforce.	• The organization can become introverted and fail to derive benefits from the public cloud and SaaS.	• Over time, there is an aggressive effort to expand and evolve this internal environment. • Organizations can selectively migrate services to external clouds as supplier offerings mature.
Cloud Only for New Systems and Applications	Legacy systems are left as they are; all new systems or applications are considered for procurement as a cloud-based service using PaaS and SaaS. SaaS may also be used as a temporary solution while the organization contemplates developing an internal solution.	• A whole new range of business models can be conceived and implemented for new business requirements, through the use of transformative cloud apps (SaaS). • Business-centric in terms of having greater affinity to the provisioning of end-user business functions through cloud-based services. • Use of SaaS and external resources can focus an organization's internal IT resources (infrastructure, people, and applications) on tasks that are critical for the enterprise.	• Potential integration challenges between new IT capabilities procured as SaaS and existing legacy applications, data, and procedures.	• The use of SaaS (within public clouds or hybrid clouds) supports the provision of rich functionality and project acceleration, leveraging the huge investments that cloud application providers make.
Composite Applications	A hybrid model that promotes composite applications that are built from multiple services from external suppliers and internal IT sources. The applications can: • Directly access Internet-located service elements • Indirectly access Internet-located services through an address managed in an internal cloud • Directly access Internet-located complete services	• Using a service may invoke a chain of sub-operations that may not all be within one supplier's cloud. The supplier could make this transparent to users by making all the sub-operations appear to be serviced from a single invocation address. Similarly, the location of an external service could be masked by an address that the enterprise owns.	• The organization must create common specifications for interfaces, protocols, and service announcements. • Also requires development and adoption of foundational cloud computing standards for identity authentication, federation, and encryption.	• Composite applications leverage different services to form an integrated business process. By composing applications from existing, prebuilt applications and services, and integrating new capabilities into existing functionality, the organization can benefit from rapid configurability and agile business workflows through the assembly of fabricated assets. The organization focuses on building and integrating what matters most to manage their restricted resources and to support business goals and initiatives. • The organization, however, needs to manage and mitigate the risk of fragile interfaces and workflows, as well as integration and quality challenges across the service chain.

The "How"

Table 18 describes various models for how cloud computing can be adopted in an organization. These models target specific "people" and change management capabilities.

In addition to the details discussed in Table 18, organizations should also consider the following:

- **Migration of Information and data to the cloud.** Various approaches are possible, including keeping the data internal and the application in the cloud, or co-locating both.
- **Where certain activities are performed.** For example, an organization could perform disaster recovery to a public or hybrid cloud, but perform production processing in the internal private cloud. However, this approach could be somewhat complex when considering complete application and systems landscapes with respect to both network configuration and data replication, which must be included and updated actively in parallel with the application systems.
- **How do deal with legacy systems.** An internal "legacy cloud" can emerge, enabling the business to access and request services from this "legacy cloud" in the same way as they request services from any real cloud service environment. This requires the cloud-based processes and control systems to be backward-integrated with the bundled legacy environments.
- **Cloud deployment options.** It may be best to start with SaaS, then integrate IaaS and PaaS as the organization's cloud adoption processes mature.

Table 18. Models for how cloud-based services can be adopted.

Model	Description	Advantages	Challenges	Outcomes
Dedicated Cloud-Force	Create and formally mandate an identified dedicated group. This group is responsible for building and establishing all cloud aspects for the organization.	• Top-to-bottom picture. • Clear objectives, timelines, and roles and responsibilities. • Reasonably fast introduction of cloud-based services and all prerequisites, with a focused pool of expertise to lead the organization.	• Resistance from existing organizations that feel threatened. • Resistance from individuals protecting legacy systems and applications. • Getting the rest of the organization to support what the cloud team introduces. • Selected systems migrate, but legacy systems may remain.	• Well-defined cloud service and strategy, with adoption concepts. • Business units can adopt these concepts, with the central team's leadership, according to their own needs.
Evolve Existing Teams	Consult with existing teams, and create a change and development plan relevant to their areas, then create a project—either a central, overall project or multiple sub-projects—that drives company-wide adoption of cloud computing.	• Entire company evolves together. • Any divisional issues are solved at a company-wide project level. • Moves slowly, but maintains momentum.	• Slow adoption rate as teams investigate issues, make decisions together, then act. • Teams are impacted by other ongoing business projects, reducing centralized focus and priority.	• Complete company-wide adoption and acceptance, with slow system migration and minimized remaining legacy environments.
Islands	Selected sections of the organization (typically those with a high change rate, such as marketing and product development) adopt cloud computing. These sections serve as leaders and mentors for other sections of the organization, who slowly leverage what the early adopters have initiated.	• The divisions that most need cloud-based services fund them and adopt them with passion, enabling others with lower priority to follow.	• Integration and management of risk and compliance requirements. • Some business units may not follow another unit on principle and so some islands may end up being left behind until "forced" to reconsider.	• Islands of expertise and adoption evolve and grow, with other islands of legacy remaining in between them. • IT needs to work closely with these units and remain in control without stifling their speed and momentum, while slowly relinquishing traditional roles and phasing into a service management role.
Cloud Broker	Contract or integrate with a cloud broker, which interprets or finds the appropriate services to fulfill defined service demands. This process occurs in a transparent manner to the organization and is typically owned by the IT and governance organizations.	• Transparent adoption and integration of cloud-based services. • Transfers much of the partnership work into a single focused area. • Helps standardize differently advertised service offerings from multiple suppliers.	• May require deployment of a broker agent. • May reduce transparency of available services. • May reduce transparency of the decision and selection process. • Depending on the completeness of the demand, may eliminate viable options early on, which the business may otherwise have adapted to.	• Results in a centralized process and controls, using a trusted party. • The cloud broker may be internal or external, and brokers relationships with commercial, service, and technical cloud service providers, taking advantage of the broker's contractual relationships.

MEASURING BENEFITS AND GOVERNING THE STRATEGY

To gauge how well cloud-based services help an organization to achieve its objectives, and to measure the organization's scale of adoption, some measurements must be defined. These measurements should be identified in the cloud strategy, so as to provide subsequent documents with a central reference. The measurements also identify how long it will be before the organization expects to realize the benefits from cloud-based services.

Key Performance Indicators

Measurements may be represented by means of KPIs, which are control tools designed to allow the measurement of some of the following in the context of an objective state:

- Progress
- Compliance
- Effectiveness
- Efficiency
- People

KPIs usually also include the dimensions of cost, time, and quality in the KPI calculation input, and initial integration measurements for cloud-based services can include percentage adoption, service performance, flexibility increases, and new product or project timeline reductions.

The measurement of the five aspects stated above is important to control, assess, and improve the status of an initiative and hence the service(s) delivered through the initiative. It is important to understand that KPIs are defined and employed within the context of a metrics tree, which originates at the company vision and goals, as shown in Figure 8.

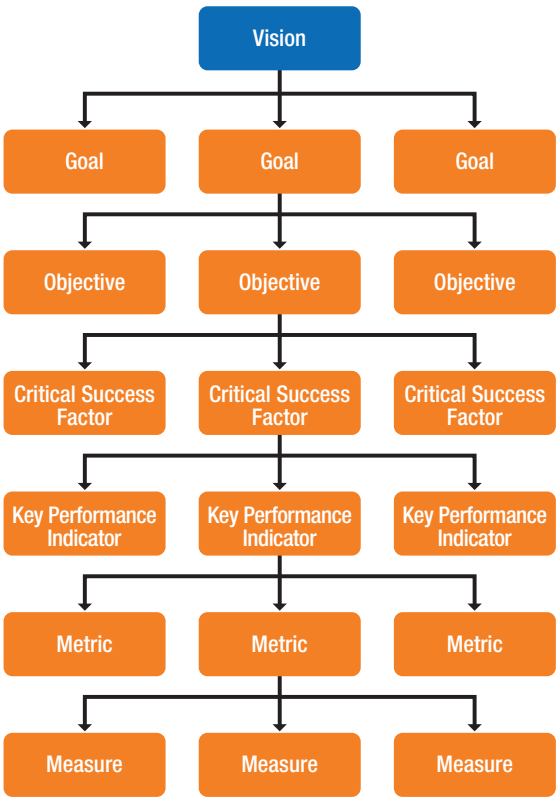

Figure 8. A metrics tree.

A KPI has the following five basic elements:

- A basic and clear statement of the KPI
- A formula for the calculation of the KPI
- Suggested targets and threshold percentages
- A statement if within the targets
- A statement if below/outside of the targets

As described in Figure 9, and within the context of the cloud strategy, the vision for cloud services integration measurement is suggested as the following:

"To support the effective and efficient integration (by a cloud service subscriber) and delivery (by a cloud service provider) of (cloud-based) services to meet the stated requirements of a cloud service subscriber."

Within the context of the cloud strategy, the following KPIs are suggested to control and measure key aspects of cloud-based service integration and delivery. Additional KPIs may be defined as the organization makes more progress toward adopting cloud-based services.

- Service availability
- The speed/timeliness of execution
- The accuracy of the expected outputs
- The compliance of the orchestrated service output(s) with applicable legal and regulatory constraints
- The (financial) cost service orchestration/execution/decommissioning
- Cloud subscriber satisfaction
- Service Execution Incident Business Impact Ratio
- People development, in the context of cloud-based services

Tables 19 through 26 describe these suggested KPIs for cloud service adoption.

While these tables represent a framework for some initial example KPIs, several other interim or additional KPIs for business-specific objectives and their achievement as appropriate to the specific business and industry sector can be determined.

Table 19. Service availability enabled by cloud.

KPI Parameter	Parameter Value
KPI Statement	Average availability of all cloud services initiated by a cloud service subscriber.
KPI Calculation Formula	$\frac{\textit{Number of cloud services meeting availability targets}}{\textit{Total number of cloud services}} \times 100\%$
Suggested Targets	• Target = 100% • Threshold = 90%
If Within Targets	Cloud-based services are available at levels that meet business needs.
If Below Targets	The services provided by the cloud service provider(s) are providing little value and, in extreme cases, could be putting the cloud service subscriber's business revenue and reputation at risk.

Table 20. Speed of service execution.

KPI Parameter	Parameter Value
KPI Statement	Percentage conformance of the speed of execution of a service against the published metrics.
KPI Calculation Formula	$\frac{\textit{Number of milliseconds for atomic cloud service execution}}{\textit{Published time (milliseconds) for atomic cloud service execution}} \times 100\%$
Suggested Targets	• Target = 100% • Threshold = 110%
If Within Targets	Cloud-based services are executing within time periods that meet business needs.
If Below Targets	The services provided by the cloud service provider(s) are taking longer than expected to execute and could, in extreme cases, be placing time-critical business services at risk.

Table 21. Accuracy of service execution.

KPI Parameter	Parameter Value
KPI Statement	Conformance of the actual service output(s) against published output(s).
KPI Calculation Formula	Comparison of the actual service output(s) to the published service output(s) to assess conformance.
Suggested Targets	• Target = 100% conformance • Threshold = Any non-conformance/unexpected service output(s)
If Within Targets	Cloud-based services are accurately delivering the outputs as published by the cloud service provider.
If Below Targets	The services provided by the cloud service provider(s) do not conform to their service publication. The published services are therefore not delivering the required value and can put the business at risk.

Table 22. Legal/regulatory compliance of service output(s).

KPI Parameter	Parameter Value
KPI Statement	Conformance of the service output(s) with predefined and applicable legal and/or regulatory constraints.
KPI Calculation Formula	Comparison of the actual service output(s) with the legal/regulatory constraint model(s) to assess conformance.
Suggested Targets	• Target = 100% conformance • Threshold = Any non-conformance of service output(s) with legal/regulatory constraints
If Within Targets	Cloud-based services are operating in a legal/regulatory conformant mode.
If Below Targets	The services provided by the cloud service provider(s) do not conform to the applicable legal/regulatory constraints and hence service operation must cease immediately until conformance is established and verified.

Table 23. Cost of service execution.

KPI Parameter	Parameter Value
KPI Statement	The percentage conformance of the actual cost of service delivery with the published price list.
KPI Calculation Formula	$\frac{\textit{Actual cost of service delivery}}{\textit{Published (expected) price for service delivery}} \times 100\%$
Suggested Targets	• Target = 100% • Threshold = 110%
If Within Targets	Cloud-based services are executing within the agreed-upon price list parameters and allocated budget.
If Below Targets	The costs for service execution are exceeding the allocated budget and the published price list and are hence not delivering the proper value for the investment.

Table 24. Cloud subscriber satisfaction.

KPI Parameter	Parameter Value
KPI Statement	Average cloud subscriber satisfaction survey score for cloud services.
KPI Calculation Formula	Average cloud subscriber satisfaction survey score.
Suggested Targets	• Target = 10.0 • Threshold = 9.0 *Assumes a 10-point scale, 10 = high and 1 = low*
If Within Targets	Cloud-based services are effectively meeting the stated needs of the cloud service subscriber.
If Below Targets	The services provided by the cloud service provider(s) are viewed as problematic, resulting in the cloud service subscriber's lack of confidence in the cloud service provider(s) capabilities.

Table 25. Cloud service execution business ratio (cloud-based compared to total landscape).

KPI Parameter	Parameter Value
KPI Statement	Business ratio for cloud-based services.
KPI Calculation Formula	$\frac{\textit{Number of cloud-based, business-level applications}}{\textit{Total number of business-level applications}} \times 100\%$
Suggested Targets	• Target = 100% • Threshold = 90%
If Within Targets	Business applications are taking advantage of cloud-based services and are meeting business needs.
If Below Targets	The projects to migrate selected business applications to cloud-based services are not achieving objectives and in extreme cases could be putting the cloud service subscriber's business revenue and reputation at risk.

Table 26. People development in the context of cloud-based services.

KPI Parameter	Parameter Value
KPI Statement	People-based capability development for cloud-based service delivery.
KPI Calculation Formula	$\frac{\textit{Cloud skills development course completed}}{\textit{Total number of cloud-based training events planned per year}} \times 100\%$
Suggested Targets	• Target = 100% • Threshold = 90%
If Within Targets	The cloud service training and development plan is on track and meeting business needs.
If Below Targets	The cloud service training and development plan is not being delivered and could be delaying cloud service adoption, thereby putting business revenue (of cloud service subscriber) and capability at risk.

Governance and Controls

"Governance" is the strategic task of setting the organization's goals and direction, specifying limitations, and establishing and accountability frameworks. In contrast, "management" is the allocation of resources and overseeing the day-to-day operations of the organization. This section considers that effective governance is necessary to maximize the achieved benefits of cloud-based services.

Ongoing attention is needed at a number of levels to direct, track, and manage the evolution of adopted cloud-based services. To do this, an organization could leverage existing forums and structures, although these may need to be enhanced to include some of the special dimensions that cloud-based services introduce. For example, the adoption of cloud-based services can drive requirements for quicker decision making. This governance update is similar to many of the functions and forums that organizations put in place to manage any other outsourced service or relationship.

Therefore, having these forums paying active and regular attention to the cloud initiative's progress will place the correct parties in control of the cloud adoption process from the beginning.

An example governance structure is depicted in Figure 9. From within this structure, the required contracts, OLAs, and SLAs are managed, commercial aspects are administered, and planning and operational communication and prioritization are performed. In the diagram, the Strategic, Tactical, and Operational layers represent different types of decisions:

- **Strategic.** Decisions relating to partners, direction, and business enablement
- **Tactical.** Decisions regarding implementation and timing
- **Operational.** Administration and execution of the strategic intent

Establishing an effective governance structure will assist IT and its supporting functions to proactively lead the business in cloud-based service adoption.

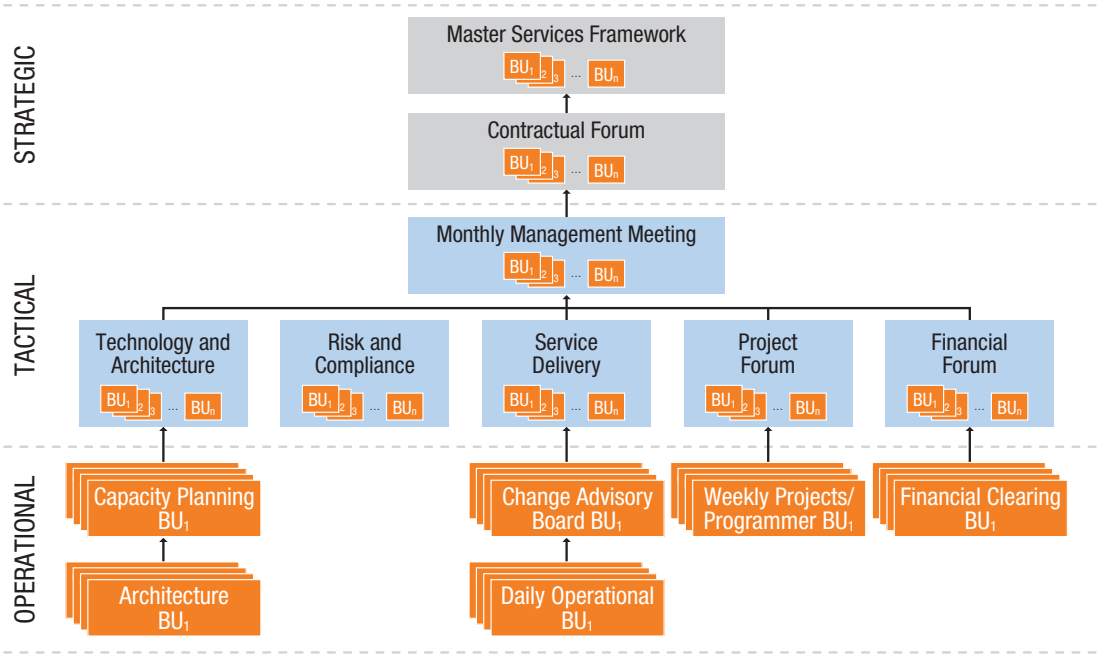

Figure 9. Example governance structure.

Governance Participation

It is important for all organizational and service provider members to participate in the appropriate governance structures at the appropriate levels. The context of participation is represented in Figure 10 from the Gartner Organization's Framework for Outsourcing, which identifies important core processes related to strategy, relationship, and management elements that must be integrated into the governance framework and into the defined mandates of each forum.

Actual interactions and responsibilities at the governance and service management relationship level could be represented as shown in Table 27, where the various forums (from Figure 10) are listed and their responsibilities identified. The content of the line next to each forum identifies the recommended mandate of that particular example governance forum, in the context of the core governance principles depicted in Figure 10.

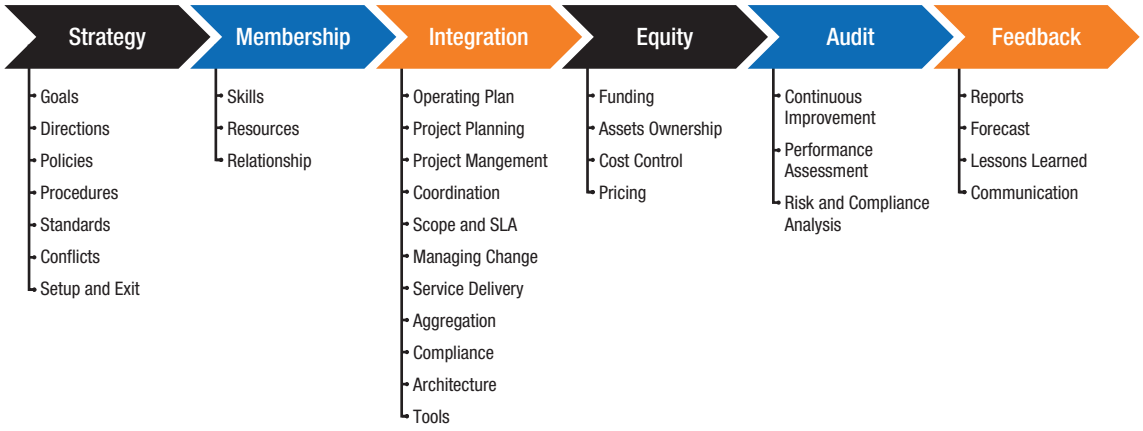

Figure 10. Context for governance participation.

Table 27. Interactions and responsibilities at the governance and service management relationship level.

		Key Relationship and Service Delivery Principles					
		Strategy	Membership	Integration	Equity	Audit	Feedback
Governance	Rolling Account Plan	• Goals	• Relationship	• Managing change	• Funding feedback • Cost control feedback • Business-case realization	• Deal evaluation • Assessment risk	• Communications • Reports
	Monthly Management Meeting	• Conflict resolution	• Relationship	• Managing change	• Funding • Cost control • Business-case realization	• Performance assessment • Risk	• Communications
	Service Forum	• Policies • Procedures • Transitions • Exit management planning	• Skills • Resources	• Delivery • Operational plan • Service levels • Coordination • Optimization planning	• Cost control • Pricing	• Performance assessment • Continuous improvement • Risk	• Reports • Lessons learned • Forecast • Communications
	Architectural Forum	• Policies • Procedures • Directions • Standards	• Relationships • Specialists	• Capacity planning • Optimization planning • Innovation planning • Technology planning • Roadmap planning	• Cost control • Cost planning • Cost avoidance • Business case development	• Risks • Business-case realization • Roadmaps • Planning	• Forecasts • Reports • Communications • Roadmaps
	Projects	• Directions • Standards	• Skills • Resources	• Project planning • Project management • Coordination	• Cost control	• Risks	• Reports • Communications
	Contractual Forum	• Transition • Exit management	• Relationships	• Scope and SLAs	• Cost control	• Risks	• Reports • Communications
	Financial Forum	• Policies • Procedures		• Managing change • Optimization	• Cost control • Asset and ownership • Pricing • Budgeting	• Risks	• Reports • Forecasts • Communications
	Daily Operational Forum	• Manage issues • Discuss issues	• Skills • Resources	• SLAs		• Risks	• Reports • Communications
	Service Quality Meeting	• Manage issues • Discuss issues		• SLAs		• Risks • Performance assessment	• Reports
	Financial Clearing House				• Funding	• Risks	• Reports
	Capacity Planning Meeting	• Planning review		• Capacity planning • Optimization planning	• Cost avoidance • Planning	• Risks • Planning	• Forecasts
	Change Management Forum					• Risks	

Governance Review

Apart from containing the IT environment within its planned scope and protecting existing investments, the governance structure must be very clear, as well as specific to the business units so that it adheres to the overall cloud strategy. The governance should protect the enterprise against cloud sprawl, scope creep, and shadow IT occurrences. A traditional organization's IT organization predetermines what business systems and data may be deployed where. In the context of cloud-based services, much more control often migrates to the business units, who take advantage of services using cloud self-service portals. (For more discussion of this topic, see the Shadow IT Prevention section.)

It follows that audits and reviews should be conducted on a regular basis, against a framework of deliverables (SLAs), rules, and guidelines (and at increased maturity levels, applied using automated tooling). These rules and guidelines are usually extrapolated from comparing application and data categorizations against business compliance requirements to determine whether what has been deployed is compliant or if there are gaps, and how the various governance forums should handle these gaps. During these reviews, multiple viewpoints should be included to ensure that the guidelines remain up-to-date and that the governance structure retains control of cloud-based service adoption (thereby avoiding difficult recoveries later). It is a significant advantage if the organization can automate the collection of underpinning information to support governance reviews.

RFP REQUIREMENTS

Following are requirements that the ODCA suggests should be included in requests for proposals (RFPs) to cloud service providers so that proposed solutions deliver services and solutions that enable an organizations' cloud strategy. Depending on whether the organization is prepared to openly share its cloud strategy document with suppliers, partners, and the public, some of the following RFP questions may be applicable or useful to consider:

- **ODCA Principle Requirement.** All services or solutions must demonstrate their ability to measurably fulfill or foster the businesses' defined objectives (the identified and relevant ones) in the context of the services being requested, as described in the organizations' cloud strategy, and commit to providing ongoing reporting in this context.
- **ODCA Principle Requirement.** Potential solution providers must demonstrate their ability to integrate with and support the organization in the context of each of the key dimensions identified in the organizations' strategy document (for example, procurement processes, capacity planning, and commercial frameworks).
- **ODCA Principle Requirement.** Services or solutions must demonstrate the level of cloud maturity they are designed to foster and also identify any investment (or savings) and effort that would be necessary to achieve higher or lower maturity levels for that component (for example, procurement integration, automation of policy enablement, and service integration levels).
- **ODCA Principle Requirement.** All potential cloud service providers must identify their ability to integrate with the company electronically, at technology, service, and commercial levels, in order to share data and reporting to create transparency into provided cloud-based services, and thereby assist in the organization's governance, risk, compliance, and associated controls.

The ODCA's online Proposal Engine Assistant Tool (PEAT)[7] can help organizations detail their RFP requirements.

[7] www.opendatacenteralliance.org/ourwork/proposalengineassistant

SUMMARY OF INDUSTRY ACTIONS REQUIRED

This document describes how an organization can foster business transformation by implementing a formal strategy for adopting cloud-based services. It also provides a summary of requirements for the cloud service provider and solution provider communities to consider when delivering cloud-based services. The ODCA Business Transformation Working Group provides this document as a way to fostering collaboration between cloud service and solution providers and organizations who want to adopt cloud-based services. This collaboration leads to an open, interoperable, and thriving ecosystem of cloud-savvy businesses and cloud-based services that contribute to the success of those businesses.

The following actions are required by the combined solution provider/consumer community:

- Classify services and options in the context of prerequisites for consumer adoption. These prerequisites should be organized by cloud maturity level, showing the differences between the levels and the advantages and disadvantages associated with adopting each maturity level.
- Define the activities, potential costs, and development requirements for all impacted elements that are needed to advance between the cloud maturity levels.
- Prepare to present services in the context of the business and with measurements including reporting of business goal and objective enablement. In other words, selling cloud-based services is transforming from an IT-level activity to a business-level activity.