VIDERITY

STRATEGIC, CREATIVE, TECHNICAL

Cloud Governance & Management Success Plan

Viderity Inc

Table of Contents

Acknowledgements

Table of Figures

Table of Tables

Chapter 1: Introduction

Information Technology (IT) related governance is a comprehensive and complex discipline. Multiple theories on IT and business alignment, the use of Balance Score Cards (BSCs) to align goals, analysis of business units and product lines in strategy formulation, and an array of standards and frameworks all add to the complexity. These tools and techniques are beneficial and often necessary for enterprise-level, IT-related governance. Many small and mid-sized organizations find enterprise-level techniques overwhelming and impossible to implement given resource constraints. However, these organizations still need an effective way to govern and manage IT. With the emergence of cloud computing the need for efficacious management and control has taken on an increased significance, particularly for government organizations that have an array of security, privacy and regulatory concerns.

This plan provides a practical step-by-step approach to constructing and implementing a Cloud Governance and Management System (CGMS) that is effective and size appropriate. The techniques presented are intended for use by small and mid-sized organizations, both standalone organizations and those within larger enterprises. The goal is to help those organizations prepare for the successful acquisition and oversight of cloud services.

Many of the approaches described throughout this plan are tried-and-proven practices implemented and refined over several years of working with businesses to define and accomplish technology-related process improvements. Other approaches expand on or were inspired by the methodologies defined in Control Objectives for Information and Related Technology (COBIT) version 5, ISO 38500:2008 (Corporate Governance of Information Technology), and the Weill and Ross framework.

Chapter 2: Cloud Governance Overview

Much is unsettled and unresolved in industry when it comes to defining and standardizing cloud computing services and related disciplines. This is due in part to the many nuanced challenges, benefits, and implications of cloud computing that are still unfolding. Conversely, a meaningful amount of standardization and knowledge exists within the area of IT governance. IT governance is the parent governing body for cloud governance. In IT governance, there are two widely accepted standards/frameworks —COBIT 5 and ISO 38500.

Also, included in a shortlist of industry-recognized authorities on IT governance is the body of work produced by Peter Weill and Jeanne W. Ross at the MIT Sloan School of Management. Weill and Ross have published several articles and a book, IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, describing their research findings and related analyses. Weill and Ross (2004) summarize that effective IT governance is the single most important predictor of the value an organization generates from IT (Chapter 1, para. 8)

What is Cloud Governance?

To define cloud governance it is helpful to give it context, starting from an understanding of "Corporate Governance'' in general and "IT Governance" in particular. Cloud governance can be viewed as an extension or component of IT governance, as illustrated in Figure 1

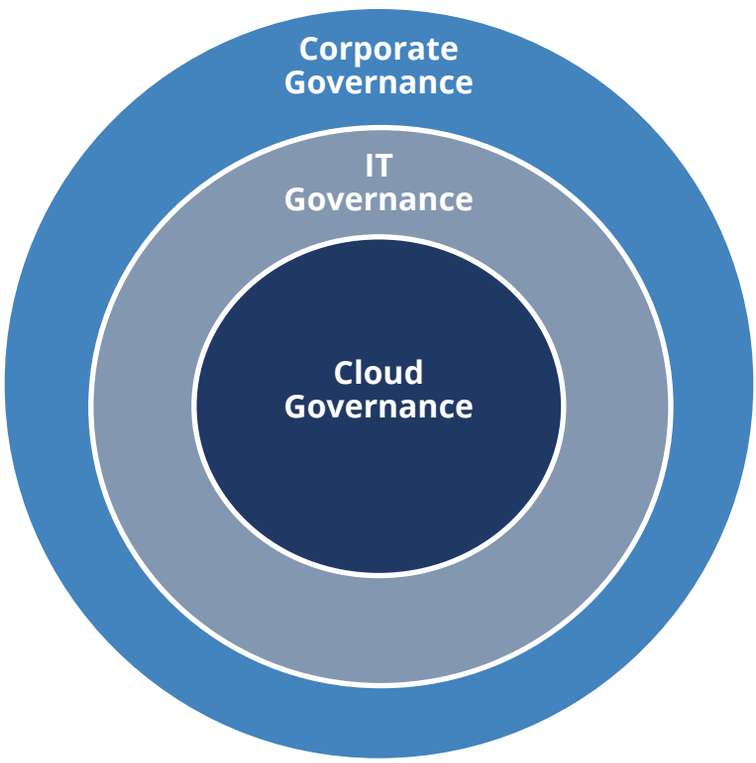


Figure 1: Context for Corporate, IT and Cloud Governance

In COBIT 5 Implementation (ISACA, 2012), Governance is generally defined as "… ensuring that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives" (p. 13). COBIT 5 goes on to identify "scope" as being important in determining the focus and size of a governance initiative.

Weil and Ross (2004) generally define governance as "specifying the decision rights and accountability framework to encourage desirable behavior" (Chapter 1, sec. 2, para. 2). The two (Weill and Ross) (2004)provide a more granular and specific view of Corporate/Enterprise Governance than COBIT 5, by identifying six key assets that should be governed – human, financial, physical, intellectual property, information and IT, and relationship (Chapter 1, sec. 1, para. 6). Shown in Figure 2, this hierarchy of responsibility, accountability, and governance domains provides a holistic view of the governance function and where IT governance fits.

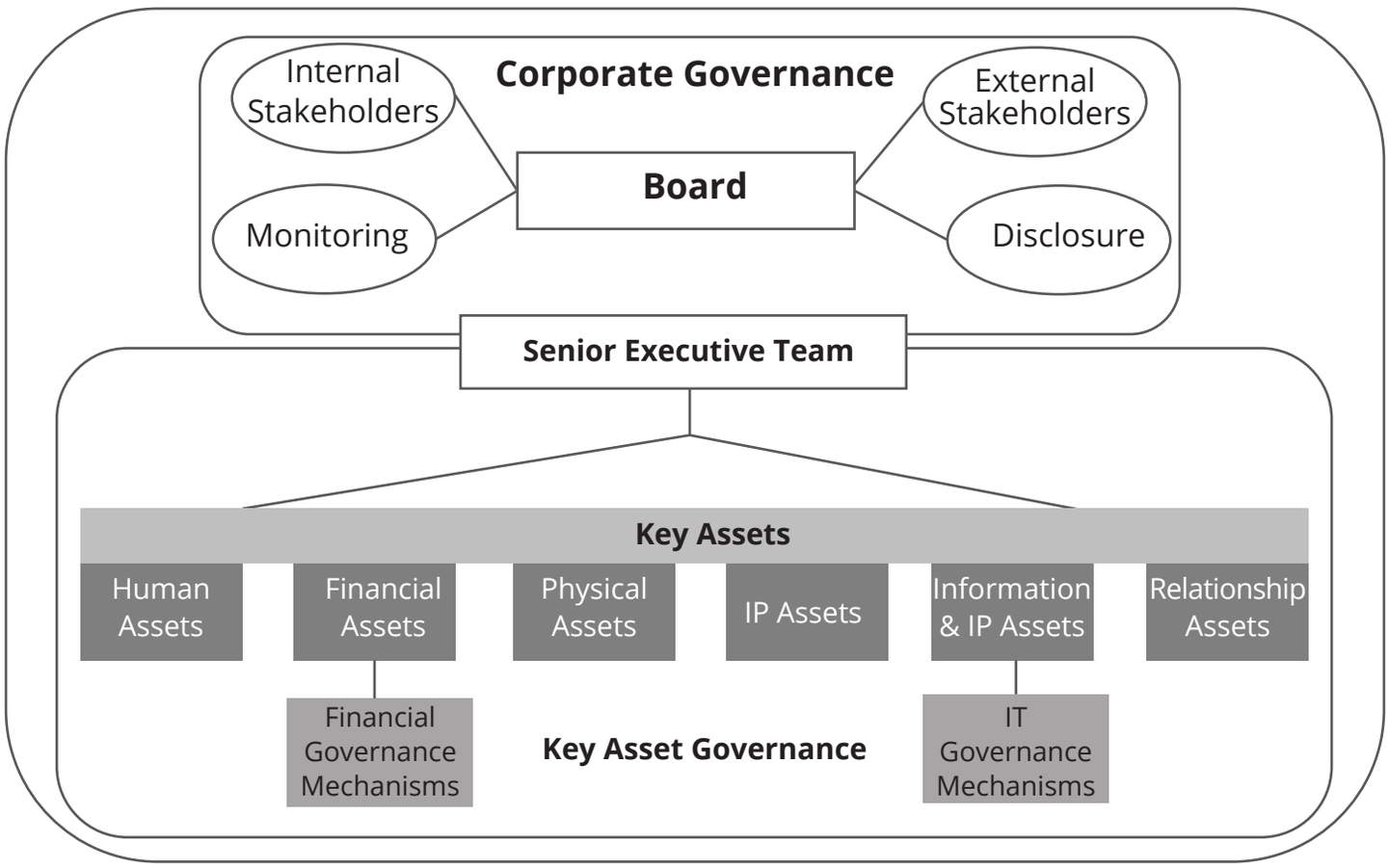


Figure 2: IT Governance Context

Source: Weil and Ross; IT Governance: How Top Performers Manage IT Decision Rights for Superior Results

If Figure 2 were further decomposed it would presumably specify what is being governed within each of the six key assets. Figure 3 takes a closer look at what is likely governed within Information & IT Assets. As shown, cloud governance can be viewed as a component of infrastructure governance, which in turn is a component of IT governance. It is noteworthy that IT and cloud governance can occur on multiple levels within an organization.

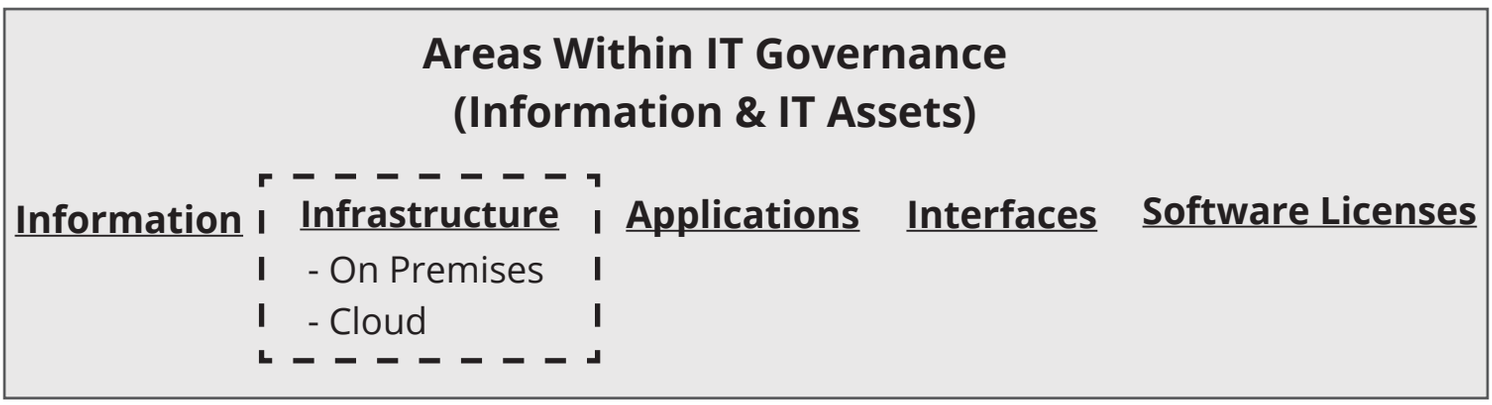


Figure 3: Cloud Governance Context

In Figure 2, Weill and Ross define "governance mechanisms" as committees, roles, formal processes and other such tools, structures, and practices necessary to perform governance. COBIT 5 makes a similar reference to such mechanisms by identifying seven governance enablers — principles, policies and frameworks; processes; organizational structure; culture; ethics and behavior; information; services, infrastructure, and applications; and, people, skills, and competencies. Enablers or mechanisms can essentially be viewed as representing the foundation necessary for effective cloud governance.

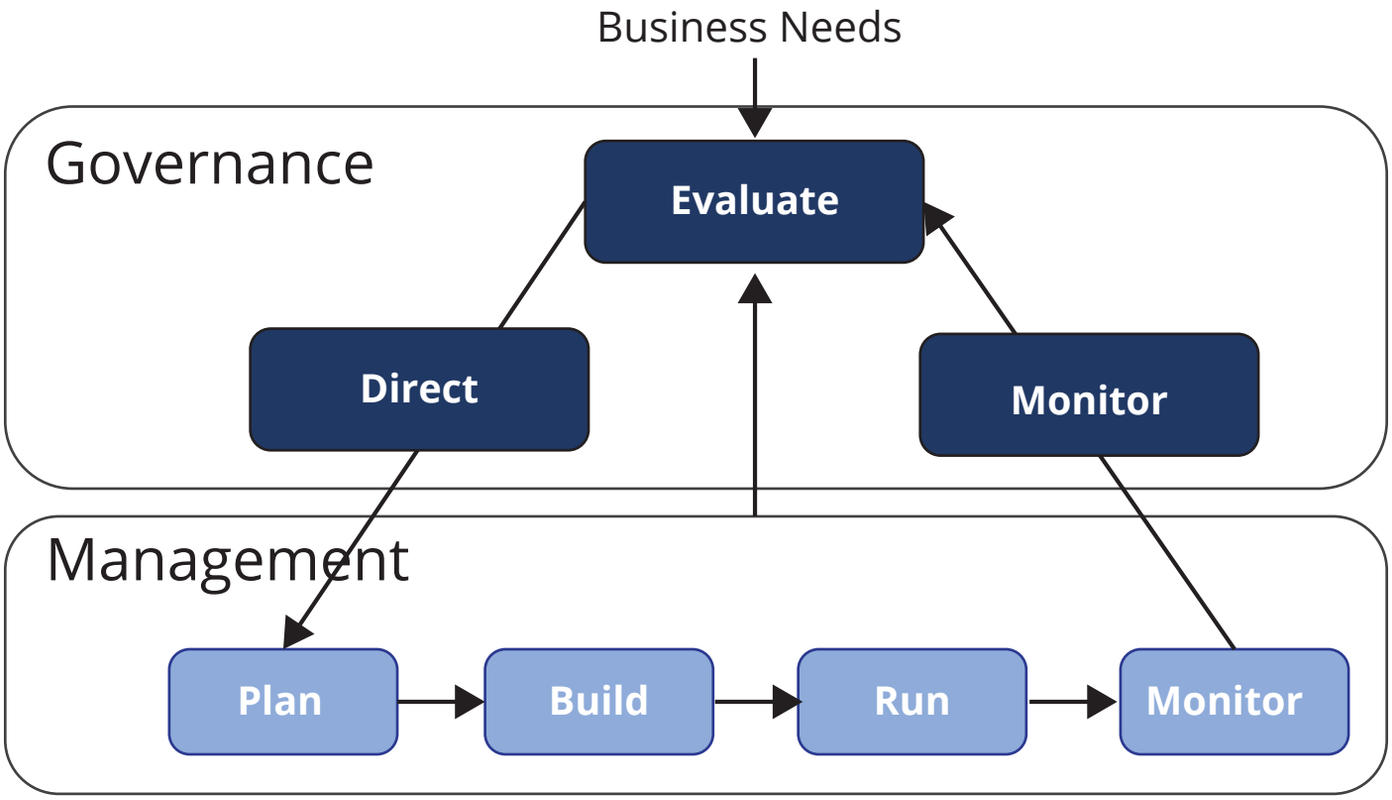
To bring the discussion full circle, what is cloud governance? Cloud governance is the subset of IT governance that embodies the tools, and capabilities needed to establish the organizational direction for cloud computing consistent with business and stakeholders' needs, and to ensure the direction is followed in a manner that minimizes risks and optimizes value to the organization.

Complexity is introduced when we began to explore the "how" of cloud governance and of governance in general. How is cloud computing direction established? How do you establish the tools and capabilities, and what are they? How do you ensure that cloud computing direction is adhered to in a manner that minimizes risks and optimizes value?

The purpose throughout this plan is to explore the "how" in as simple a presentation as possible, and in a manner that is effective and appropriate for small and mid-sized organizations.

Cloud Governance versus Cloud Management

Often the phrase "cloud governance" is used in a general sense to include both cloud governance and cloud management. However, there is a clear distinction between governance and management.
Cloud governance sets the cloud computing direction and establishes an enabling system in the organization. Cloud management uses the system to execute on the direction set by governance. Figure 4 illustrates the relationship between governance and management.



Source: COBIT 5, figure 15

Figure 4: Governance versus Management

Consistent with guidance provided in the COBIT 5 Framework (ISACA, 2012, p. 71), when considering processes for cloud service governance and management, the difference between types of processes lies within the objectives of the processes:

- Governance processes - Governance processes deal with the stakeholder governance objectives - value delivery, risk optimization and resource optimization - and include practices and activities aimed at evaluating strategic options, providing direction to cloud service initiatives and monitoring the outcomes.
- Management processes - In line with the definition of management, practices and activities in management processes cover the responsibility the typical project management life cycle (e.g., Plan, Do, Check, Act), providing end-to-end coverage of cloud services.

While separate and distinct, management and governance work together to ensure cloud-service objectives are aligned and realized.

Chapter 3: Cloud Governance & Management Considerations

If your organization already has IT governance and management capabilities, your question may be what is the big deal? Or you simply may be wondering what are the governance and management considerations associated with adopting cloud computing? To tackle these questions it is best to start from an understanding about the characteristics of a cloud service.

The National Institute of Standards and Technology (NIST) defined the following six essential characteristics of a cloud service (Hogan, Liu, Sokol& Tong, 2011, p. 14):

- On-Demand Self-Service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- Broad Network Access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and personal digital assistants [PDAs]).
- Resource Pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- Rapid Elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released too quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- Measured Service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Any service-delivery model that has the listed characteristics is likely a cloud service. The Cloud Service Essential Characteristics introduce some considerations that are different from those associated with traditional, on premises, IT Service Management (ITSM) and governance. Table 1 associates each cloud computing essential characteristic with the likely impacts it will have on conventional ITSM and governance. The impacts listed are not exhaustive, but should provide insight to some substantive considerations.

NIST Essential Cloud Characteristics	Key Impacts on Traditional ITSM and Governance
On-Demand Self-Service	• Organizations can essentially move at the speed of their processes, in particular their change management and application deployment processes. As such, agile processes will maximize the benefits of cloud computing. • The ease at which cloud resources are provisioned warrants new ways of controlling provisioning, such that resources are appropriately tracked, managed, and budgeted. • Lifecycle management of hardware is now performed by the Cloud Service Provider (CSP), to include the disposal of equipment. Gaining insight to the CSP's ITSM processes will help ensure the proper disposal of equipment, as well as other security controls used by the CSP to protect assets and data.

Broad Network Access	• Depending on the needs of an organization, the internal controls of the CSP and/or those of the organization should be able to accommodate the following: o authentication information located outside of the cloud service; o controls that account for multi-tenant environments; o as appropriate, provisioning and managing the development environment; o identity management that supports delegated authentication; and, o as appropriate, single sign-on support. • Polices, processes, and security management techniques should reflect the sensitivity of the data stored in the cloud. • Configuration, service support, and other such activities will require communication between the CSP, the on-premises IT Department, and other internal and external entities. In many cases, this communication will have to be planned, coordinated, and supported by processes, procedures, and tools. This is particularly true for service transition, and as appropriate, application migrations, and customer facing processes such as incident management. • Operational Level Agreements (OLAs) may be required to ensure internal organizations provide the required support at the desired performance levels.
Resource Pooling	• Depending on the sensitivity of the data being migrated to the cloud, security concerns and corresponding controls associated with multi-tenant cloud service models may need to be considered.
Rapid Elasticity	• There will likely be an increased importance on demand management, in particular the activities that may impact demand and hence costs. • Virtually unlimited compute and data resources can directly impact business strategies for products and services.
Measured Service	• Finance and accounting processes and practices should be able to accommo date metered services and chargebacks. • Service Level Agreements (SLAs), where possible should describe the desired service levels and penalties for missed targets.

Table 1: Cloud Service Impacts on Governance and Management

In addition to the essential characteristics presented in Table 1, NIST has also defined cloud service models and cloud deployment models. Both models (service and deployment) have aspects that impact traditional IT governance and management.

There are three cloud service models, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) (Hogan, Liu, Sokol& Tong, 2011, p. 15). Each service model provides a different scope of service to the cloud service customer. The SaaS model provides the greatest scope of service, and the IaaS model provides the least. The greater the scope of the services provided by the CSP, the greater the impact on traditional service governance and management processes. For example, if an organization plans to migrate all of its business applications to a PaaS service model, there will be a significant impact on the organization's system administration processes and procedures. Since a PaaS CSP provides and maintains the development platform and the infrastructure, many of the day-to-day responsibilities for maintaining server and network resources will be transferred to the CSP. As a result, the way the organization accounts for and manages hardware, software, and network resources will change, impacting existing processes and practices.

The extent of the impact cloud services will have on existing governance and ITSM systems, will depend in large part on the service model selected by an organization. Figure 5 illustrates the varied balance of ITSM responsibilities associated with the three cloud service models.

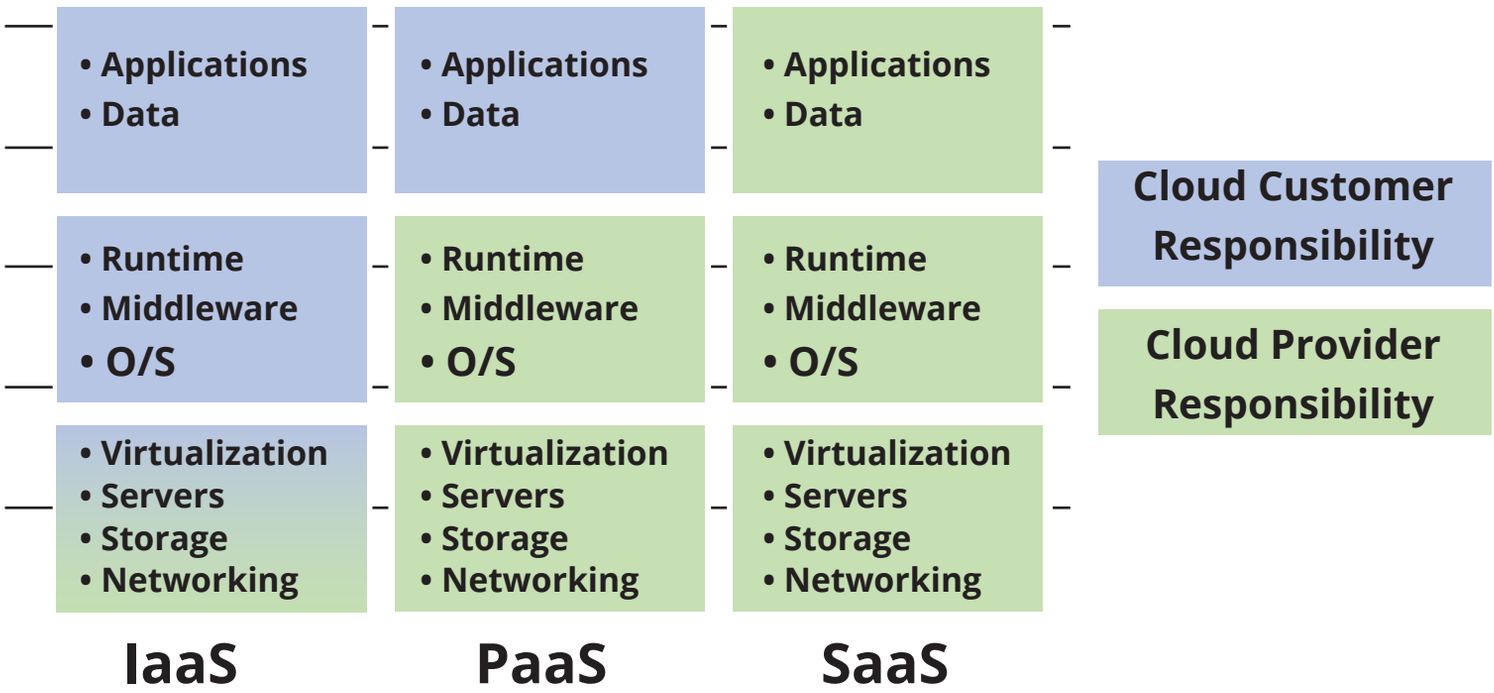


Figure 5: Cloud Service Models and Responsibilities

As shown in Figure 5, for SaaS, the CSP provides specific application services (e.g., SaleForce, MS Word, etc.) and manages the entire stack—infrastructure, platform, and application software and data. For PaaS, the CSP provides the infrastructure and the development platform. Cloud Service Customers (CSCs) can acquire PaaS services to host their existing platform-compatible applications and/or to develop new applications. Both migrated and developed applications have to be governed and managed by the CSC, as well as supplier management and oversight to ensure CSPs are appropriately performing their responsibilities.

In an IaaS configuration, the CSP provides the infrastructure (i.e., hardware, storage, and networking) and the CSC is responsible for the appropriate configuration of the infrastructure, for the configuration and management of the platform, and for the migration and/or development and management of applications. With an IaaS service model, the CSC must govern and manage all environments—infrastructure, platform, and application. All environments because in an IaaS configuration, the CSP provides the infrastructure, but it typically has to be designed and configured by the CSC. The IaaS CSP will likely provide access to virtualized storage, compute, and connectivity building blocks that have to be virtually connected and configured by the CSC. The CSC has a role in managing access and data security across all service models (i.e., IaaS, PaaS, and SaaS).

Finally, there are also four deployment models. Following is a brief description of each model (Hogan, Liu, Sokol& Tong, 2011, p. 15):

- Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
- Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Many of the governance and ITSM-related considerations associated with deployment models center on information and data security. An organization is likely to feel more secure about its information assets being maintained behind its firewall than those that are not. Other possible considerations include the location and maintenance of user authentication information, vendor lock-in, and the storage location of data.

Chapter 4: Cloud Governance & Management Approach

In this chapter, we define good cloud governance and present an approach for its design and implementation.

Good Cloud Governance

What is "good" cloud governance, and how do we achieve it? I believe most are aware of the benefits of good governance, but how does good governance look? A way to visualize good governance is to imagine an empty box. As inputs to the box, an organization has business needs, external considerations such as the competitive landscape and technology trends, and internal factors such as culture and operations' norms and challenges. Now imagine that the organization gets to decide what it would like to come out of the box, for example:

- Business needs are being met.
- Advantages of cloud services are being delivered.
- Risks are being managed and minimized.
- Stakeholders are engaged.
- Performance targets are being met.

The system of structures, controls, processes, tools and other resources an organization uses to design and construct the inside of the box such that it creates the outputs listed above is considered "good" cloud governance. There are no two organizations exactly alike. Each will have distinctive needs, risks, performance requirements, and so on. As a result, each organization's governance system will be different and consist of what is necessary for that particular organization to meet performance targets, deliver value, minimize risks (to include security and compliance risks), appropriately engage stakeholders, and meet current and future business needs.

Figure 6 illustrates the building blocks for good cloud governance. How each block is designed and implemented will depend on an organization's needs and constraints.

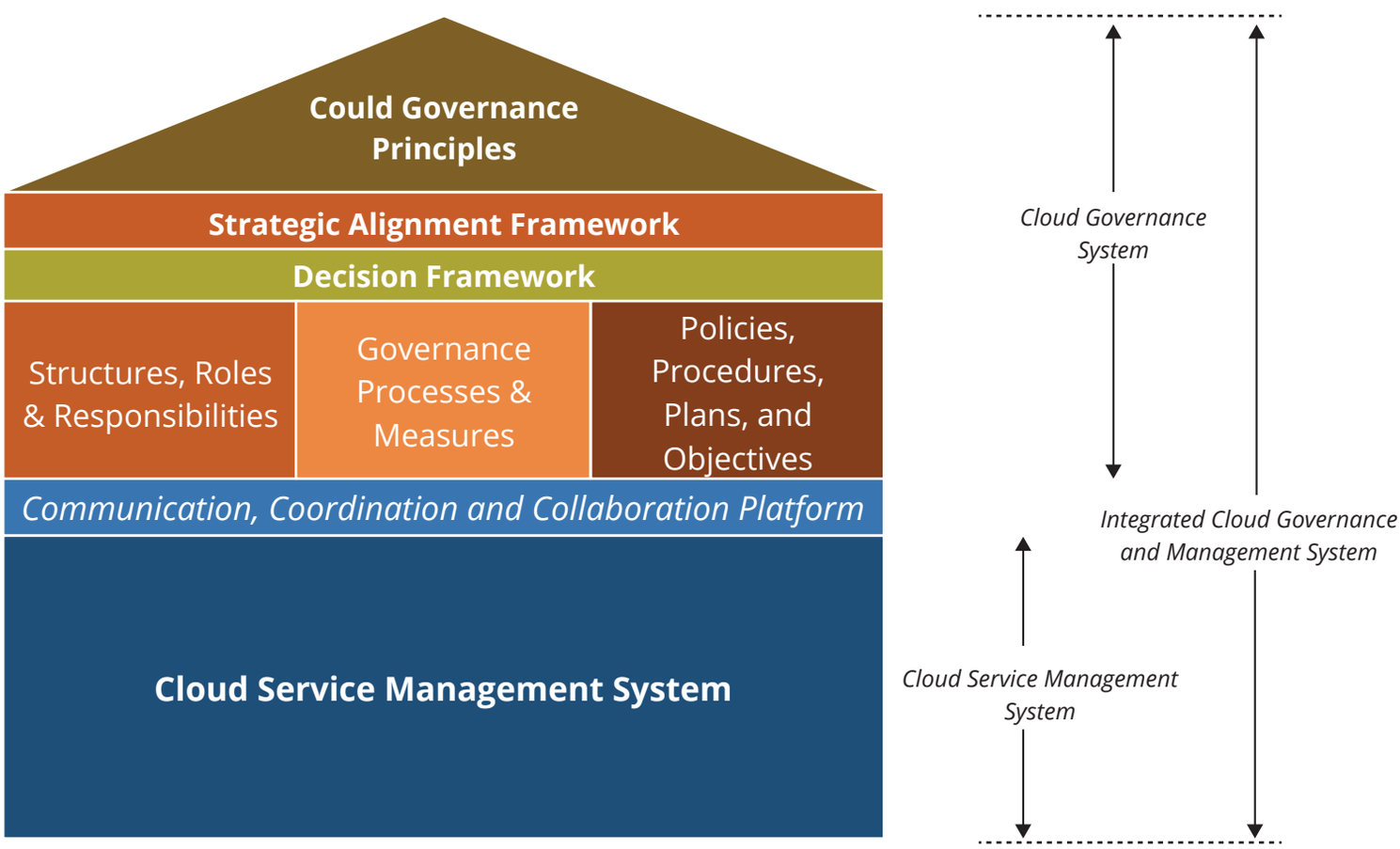


Figure 6: Good Cloud Governance

In addition to illustrating the building blocks for good cloud governance, Figure 6 provides context for the Cloud Governance System in relation to a Cloud Service Management System, and an Integrated Cloud Governance and Management System. The Integrated Cloud Governance and Management System is the sum of the individual governance and management systems. The platform shown between the governance and management systems in Figure 6, supports the integration of processes and the sharing of data and information between the two systems.

Having an integrated governance and management system is a best practice and should be considered a criterion for good cloud governance.

If your organization already has an IT governance and management system, the approach defined in the remaining chapters within this plan will provide insights on how to improve your current governance and management capabilities, and how to adapt them to better accommodate cloud services.

Practical Five-Step Approach to Good Cloud Governance

Figure 7 illustrates a five-step approach for defining and implementing an effective CGMS. The approach starts with establishing a team to plan, implement, and maintain the CGMS. The approach culminates with defining the critical success factors and key performance indicators necessary to institutionalize the CGMS. The next five chapters present a detailed discussion of each step and why the step is important.

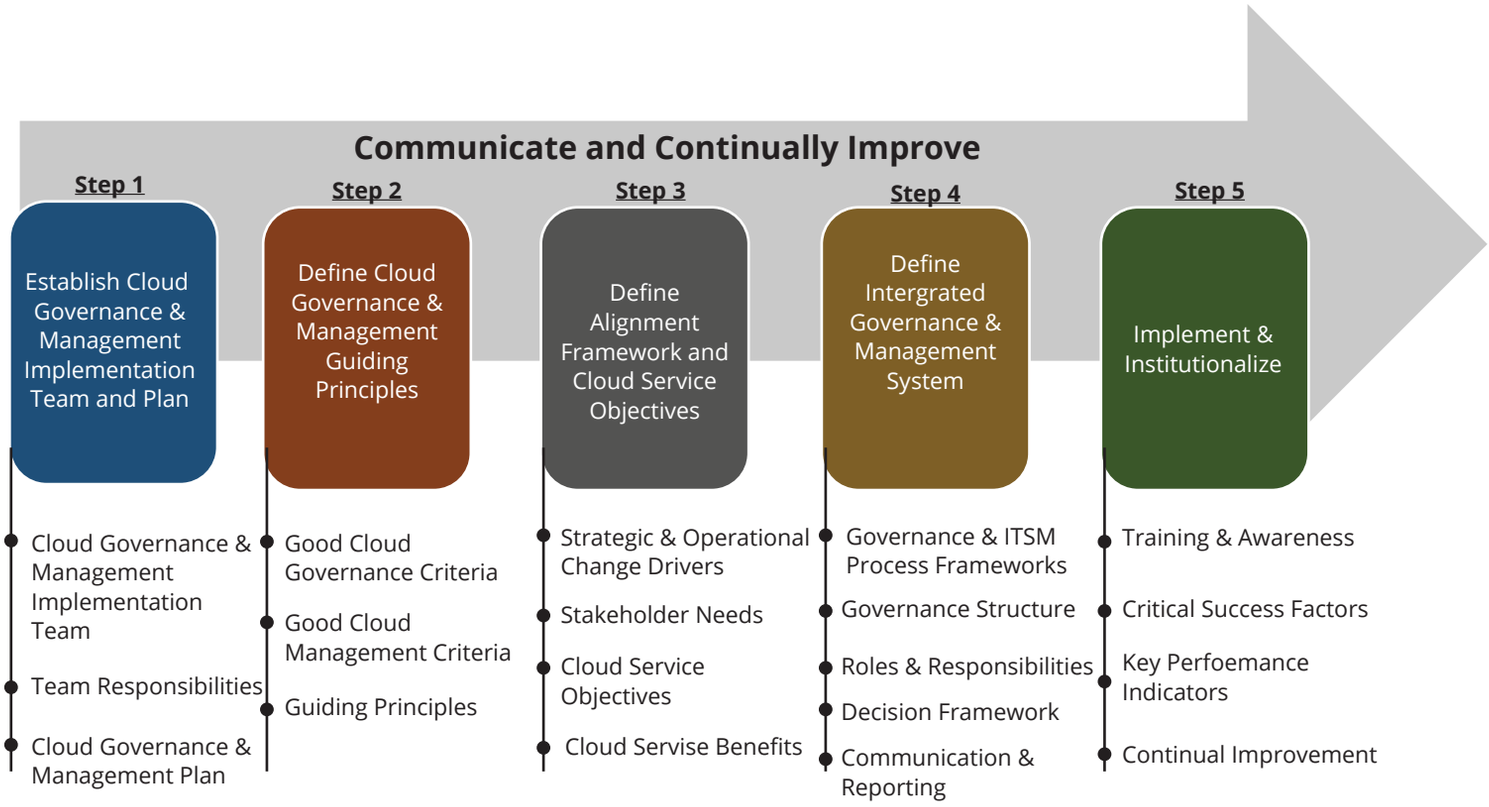


Figure 7: Five-Step Cloud Governance and Management Design and Implementation Process

Chapter 5: Step 1 - Implementation Team and Plan

In this chapter, we discuss the formation and composition of the team that will design, implement, and maintain the CGMS. As with any initiative, the development of the CGMS has to be planned and managed. Major IT initiatives often fail due to inadequate management direction, planning, and oversight. The lack of these important success drivers can result in technology adoption outpacing process adaption at the expense of operational efficiency and effectiveness.

An organization should be appropriately prepared for the adoption of cloud services. That preparation begins with an approved business case, a team to implement and support the business case, and a strategy and plan to guide the team.

Cloud Governance and Management System Implementation Team

Selecting a Team Lead and Establishing a Charter

An executive sponsor is needed for the CGMS initiative. The sponsor is typically an IT or business executive within the organization that is planning to adopt cloud services. The sponsor is responsible for selecting a team lead and working with the team lead to establish a formal charter for the team. The charter should minimally identify the sponsor, why the team is being formed, team objectives and success measures, roles and responsibilities, required team composition and matching competencies, stakeholders and corresponding areas of impact/concern, and the team communication's plan.

A team lead should be selected based on his/her or her ability to work with all levels within the organization, including executives, his/her or her cross-functional knowledge, project management skills, and facilitator skills. The team lead will work on behalf of the sponsor to establish the charter for the organization, get executive-level buy-in from business and IT, establish a coordination and collaboration platform, and recruit and train team members. Training entails making sure each team member understands the goals and objectives of the team and of the CGMS, as defined in the charter, and how to perform the tasks associated with their assigned role.

Forming the CGMS Implementation Team

The CGMS Implementation Team should be representative of the organization's varied cloud service stakeholders. The team must have both business and IT representation, and at a minimum should have three functioning tiers — executives, managers, and practitioners. Executive involvement is important for several reasons. One being that an executive committee is one of the most expeditious ways to formalize the CGMS. The executive committee should consist of the organization's business and IT leadership. Forming a committee comprised of the organization's leadership furthers the buy-in process, and streamlines communication by limiting the number of coordination points required to extract input and decisions. Further, the committee enables leadership to speak with a single voice. Among other things, this executive committee will clarify business and IT strategic objectives and provide input on how best to align cloud services with the needs within the organization.

In addition to an executive-level committee, the initiative needs a management-level coalition that formulates plans and ensures CGMS improvements are implemented. Think of this coalition as the program's Cloud Service Process Improvement Team (CPIT) responsible for overseeing the implementation of the CGMS, and ensuring that processes and other enablers are maintained and continually improved. The CPIT should convene throughout the life of cloud services to examine, identify and implement improvements to the system. Figure 8 illustrates an example of a CGMS Implementation Team. The team lead selected by the sponsor is also the CPIT Lead. The executive committee discussed in the previous paragraph is the executive arm of the CPIT or the E-CPIT. Table 2 describes the roles and responsibilities of all tiers of the CGMS Implementation Team.

As shown in Figure 8, the CPIT consists of the team lead/CPIT Lead, process area leads, and functional managers. The team is referred to as a Process Improvement (PI) Team, because the goal of the CGMS initiative is to improve existing governance and management capabilities so that they'd better support cloud

services, to include establishing new processes and capabilities. Organizations such as the Software Engineering Institute (SEI) have developed guidelines for the formation of similar teams. A well-conceived and managed PI Team is a critical success factor for the CGMS initiative, arguably the most critical.

The size of the implementation team will depend in large part on the size of the organization. A team too large will have difficulty being effectual. The goal is to have appropriate representation from both business and IT leadership, and to have productive stakeholder engagement throughout the development and implementation of the CGMS.

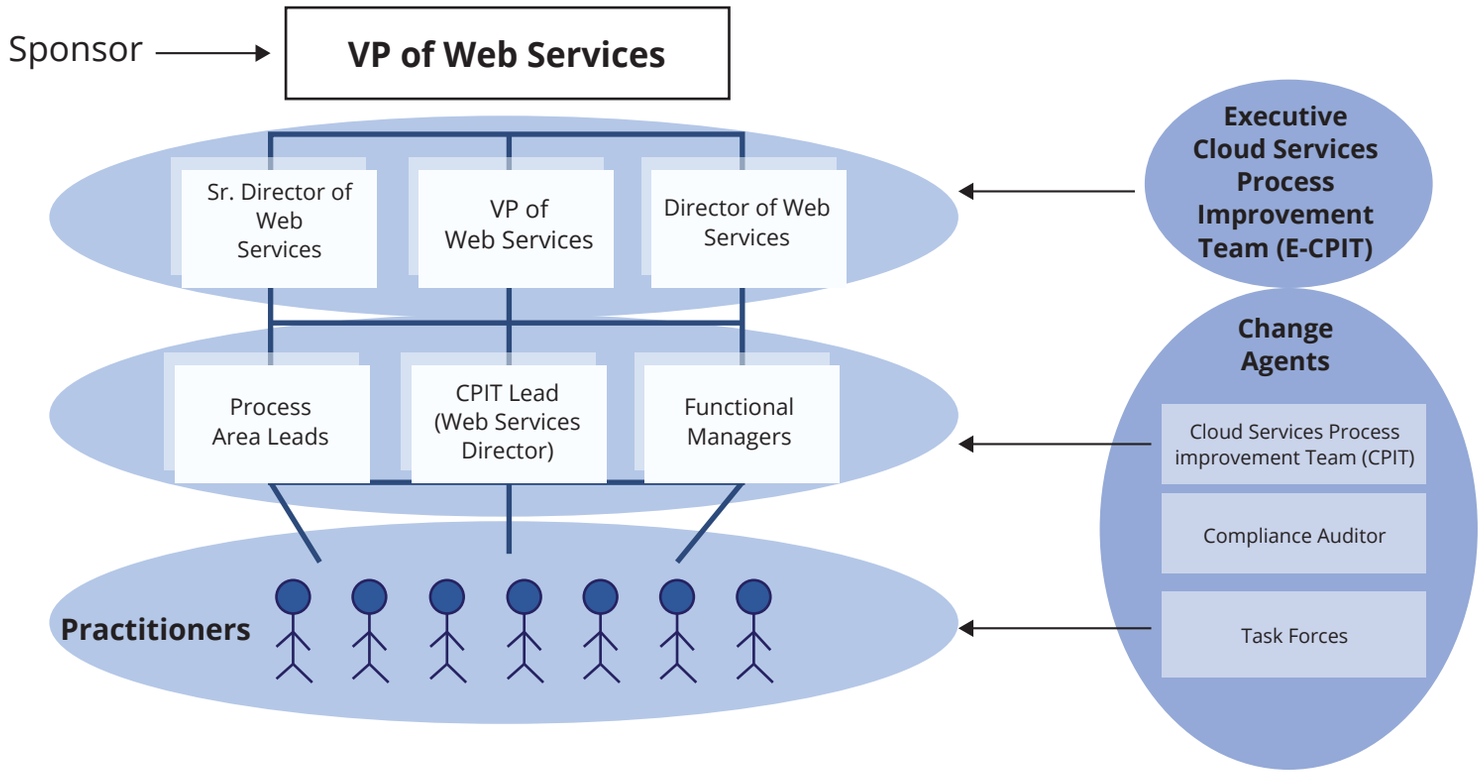


Figure 8: Example of a CGMS Implementation Team

The implementation of improved or new processes and procedures typically represents some level of organizational change, and should incorporate elements of organizational change management to facilitate and shape cultural shifts. Kotter's 8-Step Process to Leading Change, provides widely accepted guidance on organizational change management.

For smaller organizations, if the composition of the CPIT and E-CPIT is well considered, the teams can be leveraged to support cloud governance and management functions once the CGMS is implemented. For example, the E-CPIT, defined in Table 2, could reasonably also function as an Executive Cloud Governance Board since the bodies would likely have similar personnel requirements. In addition, having team members with perspectives on both cloud-related processes and operations will make the two bodies (i.e., E-CPIT, Executive Cloud Governance Board) more productive.

Role	Responsibilities
Sponsor	The sponsor ensures adequate resources for improvements and requires accountability for expenditures.
Executive Cloud Services Process Improvement Team (E-CPIT)	This group provides management oversight, approves policies, and provides overall direction. The team consists of the sponsor and the senior-most technology and business leaders within the organization. Additionally, the team supports grassroots implementation of cloud service process improvements and operates as the final approval authority for major improvements. The E-CPIT clarifies business and IT strategy and objectives and approves objectives for cloud services.

Cloud Services Process Improvement /Implementa-tion Team (CPIT)	The CPIT coordinates improvement activities and provides technical direction. The group also performs the following: • assists cloud service-related projects in identifying and implementing cloud management best practices; • develops and implements cloud service improvement plans including, developing and tracking milestones; • reports to the E-CPIT on progress against improvement targets, major issues and risks, and their statuses; and, • maintains improvement plans. The CPIT also reviews new or revised processes, approves processes for use, and manages changes to the organization's cloud governance and management process assets. The team transparently tracks and manages issues and risks to cloud service process improvement initiatives. The group consists of the organization's process and functional managers and is led by the CPIT Lead.
CPIT Lead	This individual, or his or her designee, is responsible for establishing a charter for both the E-CPIT and the CPIT, facilitating CPIT and E-CPIT meetings, preparing E-CPIT presentations, establishing the communication's plan, including meeting frequency, ensuring Task Forces are appropriately constituted and managed (e.g., objectives, tasks, timelines, etc.), documenting meeting minutes, and for tracking action items to closure. The CPIT Lead is an IT senior manager that is a member of the E-CPIT.
Task Force	These groups are temporary work groups established for the sole purpose of addressing specific objectives or improvements. Once the tasks are completed the group is dismantled. These groups are formed and managed by the CPIT.
Internal Auditor	This group or individual is responsible for assessing conformance to established governance and management processes and procedures and reporting to the E-CPIT. The Internal Auditor or group may also be responsible for assessing compliance with contractual, regulatory, and legislative requirements.

Table 2: CGMS Implementation Team Roles and Responsibilities

Cloud Governance and Management Planning

The CPIT Lead, or his or her appointee, will maintain project, objective, and policy portfolios for the team. One of the objectives in the CPIT portfolio will be to establish the CGMS. In the design and implementation of the CGMS, the first step is to define the high-level requirements and constraints for the system. From requirements, a concept of operations can be developed and agreed upon, then planning is required to document and manage the vision, strategy, CGMS objectives, Critical Success Factors (CSFs), design, implementation, and maintenance of the CGMS. The PI organization will use its teams and other resources to ensure the CGMS plan is successfully implemented.

The CPIT should routinely report progress against plan milestones to the E-CPIT.

Chapter 6: Step 2-Guiding Principles

Principles guide the design of the CGMS and define behavior expectations. Principles also provide a common thread or theme for cloud-related decisions, by providing decision makers at all levels in the organization with a shared compass.

Principles should result from an analysis of cloud computing characteristics and implications, the organization's cloud computing vision and strategy, and an understanding of the organization's culture, business strategy, mission, and values. Other components of the CGMS will echo the values defined in the principles, and the system-as a-whole will function as a magnet that pulls the organization towards a behavioral standard for cloud service governance and management.

To define the principles for the CGMS, start with defining your organization's criteria for effective cloud governance, criteria for effective cloud management, and organizational behaviors that will exemplify strategic and operational goals and objectives. For example, if an organization plans to make a major shift in its business model, and as a result has to transition from a solution-focused to a customer-focused organization, changes in organizational behavior will likely be required. The resulting target behavior should be contained in the organization's principles. Organizational behavior modifications will be encouraged through the organization's policies, processes, procedures, reward systems and other such mechanisms that follow the guidelines inherent in the principles.

In the following sections, we will walk through the process of defining CGMS principles by first defining the requirements or criteria for the principles. If your organization already has IT governance and management principles, then this exercise should provide insights on cloud-driven considerations that should be examined for potential impact on the organization's principles and practices.

Criteria for Effective Cloud Governance

Your organization will need to define its criteria for effective cloud governance.

The outputs an organization needs from its cloud governance system are based upon the needs within the organization. Since no two businesses are alike, the criteria for effective cloud governance will vary between organizations. That being said, following is a list of some core cloud-governance-system criteria that should exist for most cloud governance systems:

1. It ensures alignment of cloud services with business goals and objectives, IT goals and objectives, and stakeholder needs.
2. It ensures the appropriate cloud service-related communication and reporting.
3. It ensures cloud service acquisitions are properly constructed to meet cloud service and business needs.
4. It ensures that cloud service objectives are met.
5. It ensures agility in processes and practices to leverage fully the capabilities of cloud services.
6. It ensures anticipated cloud service benefits are realized.
7. It ensures that organizational risks associated with cloud services, including security risks, are identified, tracked, and appropriately managed.
8. It ensures that cloud service-related activities are in compliance with legislative, regulatory, contractual requirements, internal procedures, and performance targets.
9. It ensures stakeholders are appropriately engaged.
10. It ensures data and information stored in the cloud is secure.
11. It ensures teams are properly trained; individuals have the appropriate competency, and everyone is aware of their governance and management role and responsibilities.

It is recommended that your cloud governance criteria minimally include the items listed above. You should add to the list criteria specific to the needs of your organization.

The core criteria will likely evolve over time, since defining/refining cloud service principles is a living process. Having said that, principles should not be the subject of volatility, or the organization will not view the principles seriously or see them as lacking in credibility. However, when there are developments impacting the organization such as changes in business strategy, technological advances, or competitive threats, the CPIT should review guiding principles and adapt them as needed to the new landscape.

Criteria for Effective Cloud Management

Your organization's criteria for effective cloud management must support the criteria defined in the previous section for effective cloud governance. The two disciplines, governance and management, work together. A single cloud management criterion may support multiple governance criteria. Following is a list of examples of criterion for effective cloud management:

1. The system has the ability to define cloud service objectives that appropriately align with business and IT objectives and stakeholder needs.
2. The system has the ability to plan, track, manage and drive cloud service objectives to closure.
3. The system has the ability to define, track, and manage communication and reporting requirements.
4. The system has the ability to meet communication and reporting requirements.
5. The system has the ability to define and implement lean processes and procedures that are consistent with guidelines from governance.
6. The system has the ability to plan, track, manage, and drive to fruition cloud benefits.
7. The system has the ability to track and appropriately manage compliance with legislative, regulatory and contractual requirements, with internal procedures, and with performance targets.
8. The system has the ability to engage, track and appropriately manage stakeholders.
9. The system has the ability to define and manage the implementation of security controls that are appropriate for data and information sensitivity and risk levels.
10. The system has the ability to acquire the appropriate staff and to create awareness of roles and responsibilities.

As with cloud governance criteria, cloud management criteria will evolve over time. Every change in criteria does not require a change in the principles. Typically, there should be years or even decades in between changes in principles. As such adequate diligence should be applied when defining cloud principles.

Criteria for Other Desired Behaviors

We have discussed both the criteria for effective cloud governance and for effective cloud management. The other consideration when defining CGMS principles is those behaviors the organization would like to change or encourage to align behaviors more tightly with the needs of the business.

To aid your thought process concerning other desired behaviors, think in terms of the current culture and compare those organizational behaviors to the behaviors required to achieve business strategies, business and technology priorities, and other such desires that push the organization in directions different than the status quo. Remember, the goal is to have everything align with the needs of the business - objectives, behaviors, policies, and so on.

Following is a list of example criterion for other desired behaviors:

1. The organization's behavior will increase the quality and consistency of customer service.
2. The organization's behavior increases the number sales leads generated by business leads and managers.

As a checklist to help provoke a comprehensive thought process, strategic planning tools such as the BSC may be helpful.

Cloud Service Principles that Meet Criteria

Once you have defined a working list of cloud governance, cloud management, and other behavior criteria, synthesize these lists into a single list. Remember that at a minimum, your list should address the entire list of cloud governance criteria, along with supporting management and behavioral criteria. From your compiled list, develop principle statements that address all the criteria. Your principles should define a code of conduct that addresses the criteria.

Table 3 presents some examples of cloud governance and management principles. The principles in Table 3 do not directly correspond to the criteria examples used in the previous sections.

The ISO 38500 standard, Corporate Governance of Information Technology, defines six core principles — Responsibility, Strategy, Acquisition, Performance, Conformance, and Human Behavior (ISO & IEC, 2008, p. 6). Your organization's cloud service principles should echo the behaviors that are consistent with the needs of

your organization and that meet criteria. The ISO 38500 principles are recognized best practices that should be leveraged when compiling organization-specific cloud service principles.

For organizations with existing IT principles, your resulting set of principles could be two or three principles that will be integrated with your existing IT principles.

Principle	Description
Responsibility	There are clear roles and responsibilities for all CGMS-related activities. Clear competency requirements are defined and adhered to for all roles.
Accountability	There are controls and monitoring mechanisms to ensure that assigned responsibilities are successfully performed.
Acquisition	A formal process is used to acquire cloud services such that all cloud service requirements are clearly defined to include security, service continuity and availability requirements, service level targets, and corresponding chargebacks. Cloud service acquisitions are preceded by a business case, and acquisitions strike the appropriate balance between opportunity, benefits, risks, and costs.
Agility	Processes and procedures are streamlined to minimize execution time without compromising required controls.
Alignment	Business, IT, and cloud computing objectives, plans, practices, infrastructure, and stakeholder needs are aligned and consistent with the needs of the business.
Stakeholder Involvement	Stakeholders are engaged according to a documented Stakeholder Engagement Plan. Stakeholders have access to information and resources necessary to accomplish assigned tasks and make decisions.
Compliance	Services and activities comply with mandatory legislation, regulations, and contractual requirements. Activities are performed consistent with internal policies, processes and procedures.
Performance	Services and service levels are consistent with plans and agreements and meet current and future requirements.
People	All staff are aware of their roles and responsibilities and have the appropriate training and skills to perform.
Risk Optimization	Risks are identified and managed for all projects and services.

Table 3: Example Cloud Service Guiding Principles

A word of caution, as discussed in Chapter 5, while there are techniques that aid in organizational behavior modification, changing organizational behavior is a challenge at best. To the extent you can work within cultural norms to implement effective cloud governance and management, you should. However, despite your best efforts, some cultural changes will likely be necessary, particularly for new governance and management systems.

Chapter 7: Step 3-Alignment Framework & Cloud Objectives

In the previous chapter, we defined the guiding principles for the CGMS. The principles represent the characteristics that should be reinforced through CGMS tools, components, and practices.

In this step, we will define the Alignment Framework and the cloud service objectives. The Alignment Framework defines the organization's approach to aligning cloud service objectives with the organization's business and IT objectives and with stakeholders' needs. If your organization has an established strategic planning process, business and IT strategic objectives are likely outputs of that process. Those same business and IT objectives would serve as inputs to the alignment process described in this chapter. If your organization does not have a formal planning process, then ensuring that cloud service objectives are strategically aligned will require some effort to coordinate with business and IT leadership to define organizational strategic goals.

Alignment Framework

If cloud service objectives are not aligned to the needs of the business, implementing cloud computing will represent a step backwards towards unchecked IT expenditures that don't enable or support the needs of the business.

Figure 9 illustrates what is meant by cloud service alignment. The Alignment Framework provides an approach for aligning cloud service objectives with business and IT strategic objectives, with business and IT operational objectives, and with stakeholder needs.

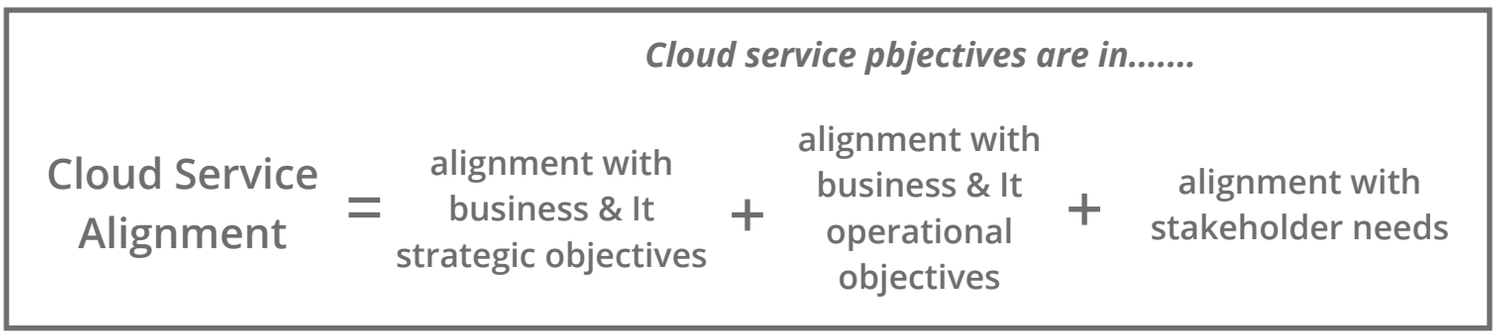


Figure 9: Cloud Service Alignment

Cloud service objectives are specific, measurable milestones that must be achieved to reach a goal defined by the organization. Defining cloud service objectives is not an event, but a continual process that must be revisited and managed. Cloud service objectives are a subset of IT objectives and are typically either strategic or operational. Figure 10 illustrations the relationship between strategic and operational objectives as discussed within this chapter. Strategic cloud service objectives support long-term business and IT strategies. Operational cloud service objectives are shorter-term, unit-level objectives that must be achieved in order to meet the longer-term strategic objectives. Operational cloud service objectives may also address operational challenges or pain points that require short term resolution.

Figure 10 also illustrates how operations' challenges can result in strategic goals for long-term solutions and/or operational objectives for more immediate remedies.

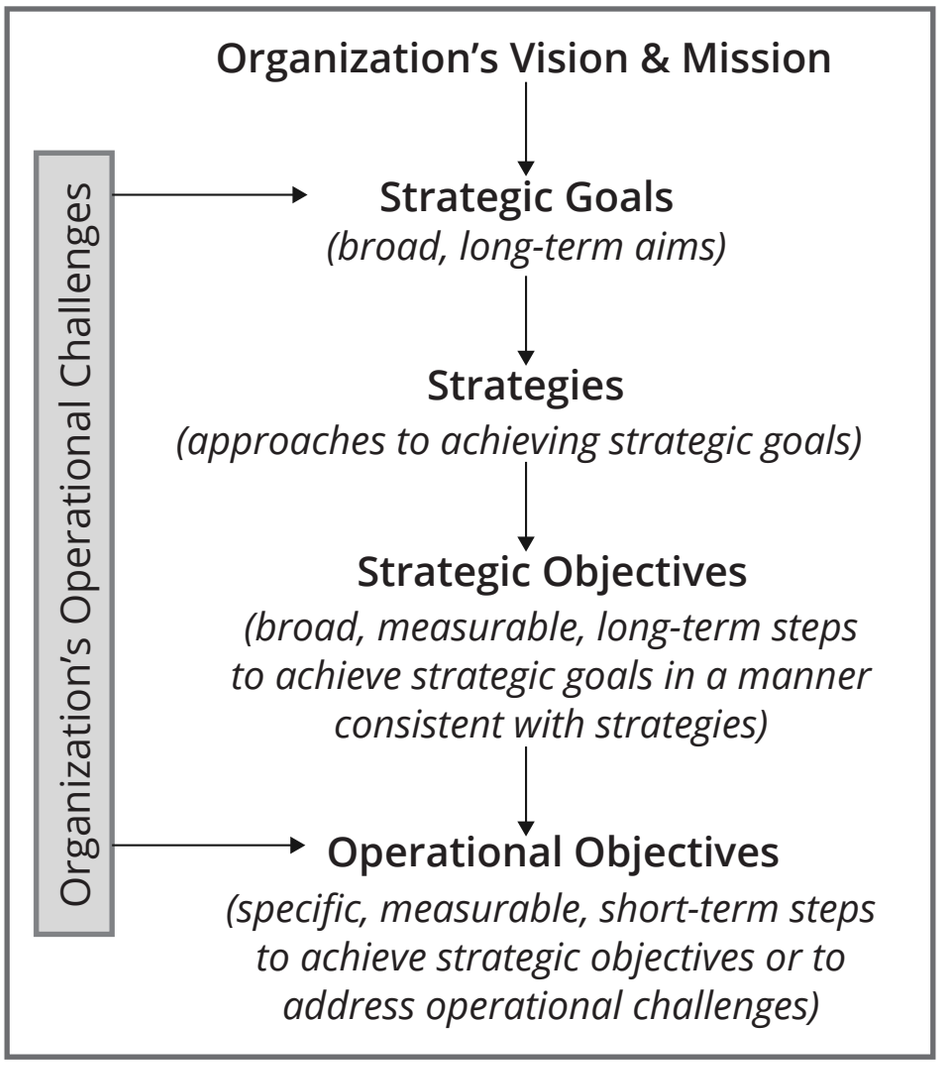


Figure 10: Relationship between Strategic and Operational Objectives

A critical role of the CGMS is to ensure that cloud service objectives, both strategic and operational, are properly defined and realized. Cloud service objectives should meet the following criteria:

- aligned with business and IT strategies and objectives (strategic change drivers);
- address stakeholder needs;
- be responsive to operational change drivers; and,
- be prioritized and measurable.

As shown in Figure 11, the key inputs to the process of defining cloud service objectives are strategic change drivers, operational change drivers, and stakeholder needs. There may be overlaps and/or synergies that naturally exist between these inputs.

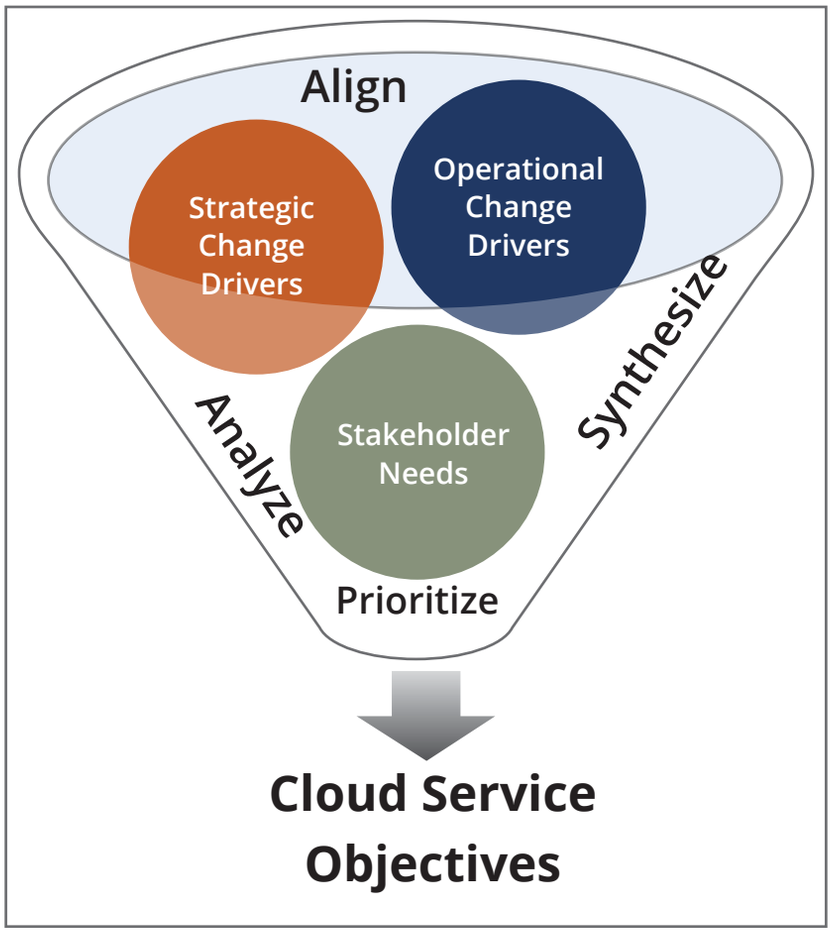


Figure 11: Cloud Service Objectives Definition Process

In the next few sections, we will examine each of these inputs (strategic change drivers, operational change drivers, and stakeholder needs) and show how their analysis yields prioritized cloud service objectives that are aligned with business and stakeholder needs.

Strategic Change Drivers and Supporting Cloud Service Operational Objectives

A change driver is an internal or external event or anticipated event that serves as the stimulus for change. Industry and technology trends, performance concerns and issues, new application requirements, and even organization-level goals can act as change drivers.

Change drivers can be further segmented into strategic and operational. Strategic change drivers typically result from executive management, ideally business and IT, completing the strategic planning process. A strategic plan and its strategic goals and objectives are strategic change drivers. Technology trends, such as cloud computing, can also be viewed as strategic change drivers. Cloud service strategic and operational objectives can result from strategic change drivers. An operational objective can be viewed as a milestone necessary to achieve a strategic objective.

Increasingly for organizations to be successful, IT initiatives have to be tightly coupled with business strategic goals and objectives. The traditional approach to aligning business and IT is for executive leadership to define business strategic goals (strategic change drivers) along with strategies for their attainment. IT would then use the business goals and strategies to define corresponding IT goals and objectives to enable and support the business goals. Since cloud services are a component of IT, cloud service objectives would be a subset of the IT objectives. However, business and IT alignment is not always driven by business.

Alignment between business and IT can occur from varied perspectives (Henderson & Venkatraman, 1993). Just as the business strategy can drive the alignment process, IT strategy can also drive the process. This IT-driven alignment is likely the case for many organizations when it comes to cloud services. The value proposition and increasing popularity of cloud services are prompting many organizations to re-tool their IT strategies around cloud computing, then work with business to determine how best to provide additional business value. When IT and business alignment are approached from this perspective, IT strategy is the driver that shapes the business strategy.

With an IT-driven strategy for cloud services, IT strategies are not bound by business strategy. As such, business goals, strategies, and objectives are influenced by the capabilities of cloud services. Cloud services provide opportunities to reduce or eliminate IT capital expenditures and virtually unlimited storage, compute, and broadband

capabilities.

Independent of the driver of the alignment (i.e., business or IT), cloud services provide IT with a powerful tool with which to form better, tighter alignment with business. Figure 12 illustrates the general alignment between business, IT, and cloud services. The alignment approach (business driven or IT driven) selected by an organization is dictated by internal and external factors, such as the organization's business needs and culture.

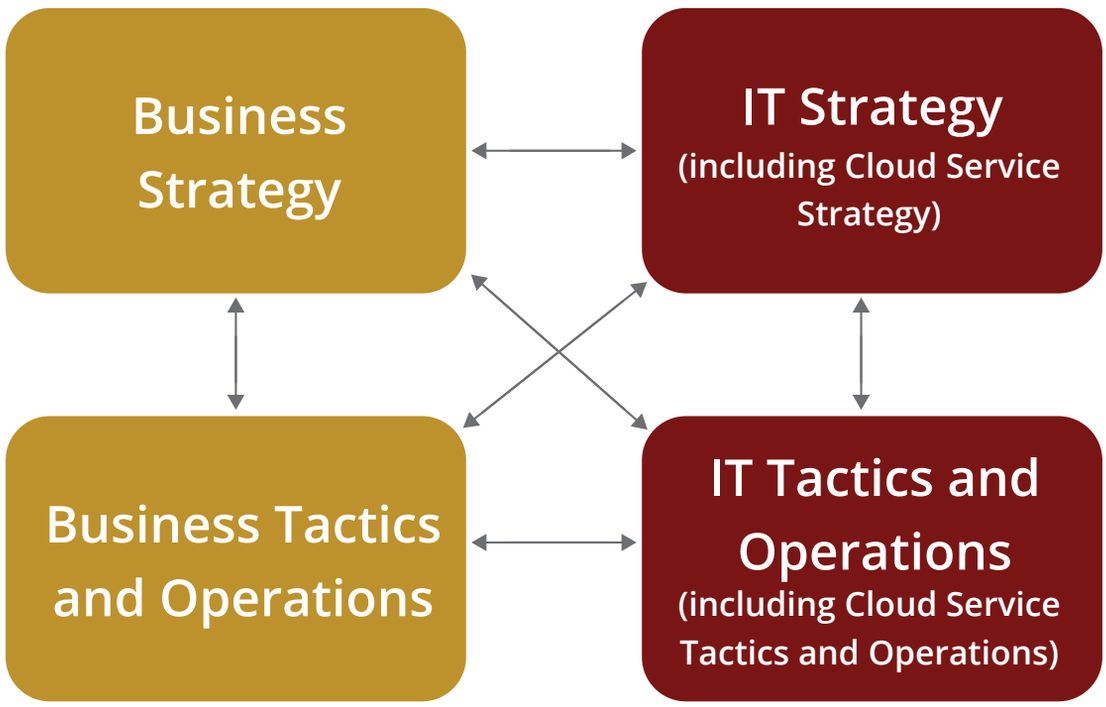


Figure 12: Alignment between Business and IT

Adapted from source: Henderson & Venkatraman, 1993

The goal of this task is to determine the cloud service objectives resulting from business and IT strategic alignment. For example, Table 4 shows a scenario in which alignment is driven by IT. In the example in Table 4, triggering events such as trends in cloud computing and increasing resource demands to support new applications influenced company AYZ's selection of an IT-driven approach.

In Table 4 goals, strategies, and objectives are defined as follows (also see Figure 10):

- Strategic Goal – a broad, long-term aim that is consistent with the organization's vision and mission.
- Strategy- the approach that should be taken to achieve objectives and to support strategic goals.
- Strategic Objective – broad, measurable, long-term step taken to achieve a strategic goal in a manner consistent with the strategy.
- Operational Objective - a specific, measurable step taken to achieve a strategic objective. Operational objectives can be viewed as incremental milestones associated with strategic objectives.
- Tactic (not included in Table 4) - a specific action taken that is designed to execute a strategy and fulfil an operational objective.

Not shown in Table 4 is the action plan or tactics for each of the operational objectives since it is beyond the scope of this plan.

As you complete the task of defining cloud service strategic and operational objectives keep in mind that cloud service objectives are components of IT objectives. As such, they will likely be interwoven into a larger set of goals and objectives that may not be specific to cloud services.

The task of defining cloud service strategic and supporting operational objective is best completed with the input of the organization's leadership, or those mindful of the organization's strategic goals and objectives. As such, the CPIT should complete this task and get input and approval from the E-CPIT. Once the cloud service objectives have been defined, the role of the CGMS is to ensure the objectives are appropriately managed and realized.

IT Strategic Goal	Strategy	Strategic Objective	Operational Objective
Establish a world-class IT infrastructure to serve as a center of excellence, to create ITSM efficiencies, and to strengthen the organization's competitive posture.	Migrate all infrastructure services to cloud computing configurations in a manner that maximizes cloud service capabilities.	• Migrate corporate infrastructure to the cloud in a manner that maximizes cloud service capabilities within one year. • Migrate data centers to cloud services in a manner that maximizes cloud service's capabilities within three years.	• Migrate Virginia corporate office to a cloud PaaS configuration by the end of 2015. • Migrate data centers AB and XY to a cloud PaaS configuration by the end of 2015. • Migrate data centers CD to a cloud PaaS configuration by the end of 2016.

Table 4: Example Cloud Service Strategy-Related Objectives

The next step is to define cloud service operational objectives that result from operational change drivers.

Operational Change Drivers and Supporting Cloud Service Operational Objectives

Operational change drivers are typically related to operational events and issues, or anticipated events and risks. If customers are continually experiencing application performance issues, this is considered an operational change driver.

To identify operational change drivers, list all known IT-related issues and risks. For the issues and risks you list, define your objectives for the solution that will ultimately address the change driver. The response to all the operational change drivers may not be cloud related; you should include them as well. At this stage within the process, it may not be completely apparent which change drivers may have a cloud service-related response.

There may be some overlap with cloud service strategic objectives, but that is ok. You simply want to identify all operational change drivers and comparable responses. Table 5 presents some examples of operational change drivers and matching response objectives. Objectives should be measurable and directly address the change driver.

The CPIT should complete this task in a group since it has a membership that is representative of the organization's business and IT managers. The CPIT may also decide to form a Task Force and include select participants who can provide the most accurate and comprehensive input.

Example Operational Change Drivers	Response Objectives
Infrastructure Performance Shortfalls: The infrastructure continually performs at unacceptable levels.	• Establish performance targets for infrastructure and platform services. • Ensure that infrastructure and platform services consistently perform within established service targets. • Establish penalties for missed service targets.
Insufficient IT Staff with Adequate Skills: The Infrastructure Team continually has difficulty maintaining skilled personnel.	• Decrease the number of skilled personnel needed for infrastructure and platform support. • Increase the skill level of those responsible for infrastructure and platform support.

Table 5: Example of Operational Cloud Service Drivers

Stakeholder Analysis

Stakeholder analysis is the process of identifying the individuals or groups that are likely to affect or be

affected by cloud services and sorting them according to impact. Understanding the stakeholder landscape is critical for the success of any initiative, particularly the establishment and operation of a governance and management system. The lack of appropriate stakeholder involvement can lead to a CGMS that falls short of the overall need. In addition, getting buy-in from stakeholders with influence or power is a critical success factor. As such, stakeholder needs must be considered when defining and analyzing cloud service objectives.

For our purposes, a simplified five-step Stakeholder Analysis Process is defined in the following steps:

1. Identify all stakeholders. When identifying stakeholders it may be helpful to use the following questions as a guide:
   - If the cloud service failed, which business processes, individuals, groups, or organizations would be impacted?
   - Within the cloud-service-customer organization, what is the chain of command in the management of cloud services?
   - Which individuals, groups, or organizations are required to establish and maintain cloud computing services and supporting configurations?
   - Which individuals, groups, or organizations are involved in establishing architecture, security, and service continuity requirements for cloud services, hosted applications, and data?
   - Which individuals, groups, or organizations are involved in support for hosted applications?

Figure 13 depicts the stakeholders for the Web Services Division of AYZ, Inc., a fictitious international e-commerce company. Internal stakeholders are being defined as those internal to the Web Services Division of AYZ, Inc. External stakeholders are those outside of the division.

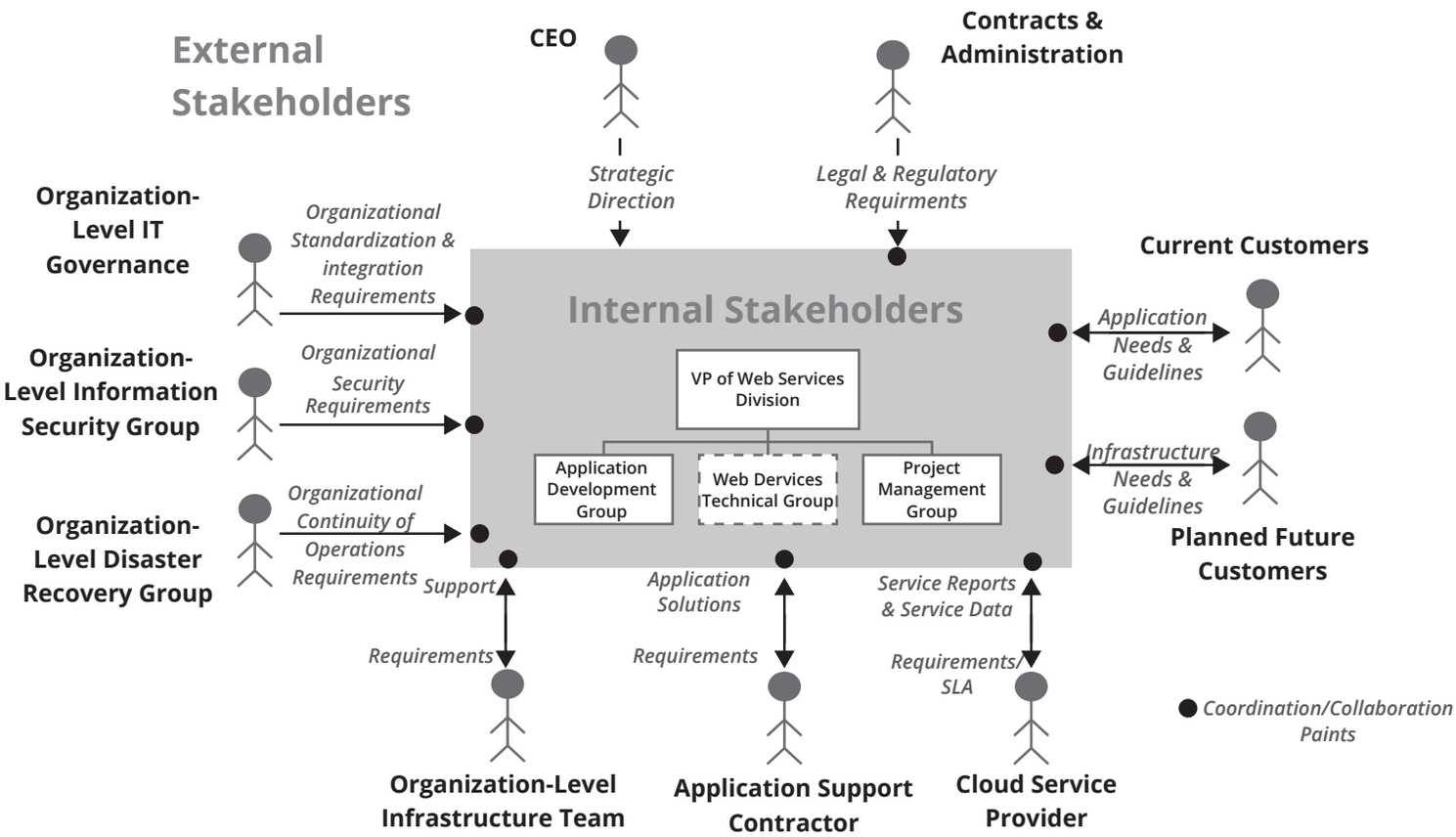


Figure 13: Example of Cloud Service Stakeholders

2. Identify the impact stakeholders will have on cloud services and vice versa. When you think of impacts, remember business processes being enabled by cloud services.

   The impact a stakeholder has on cloud services, and vice versa, will dictate how stakeholders are engaged and the flow of information between the stakeholder and the CGMS. The black dots in Figure 13 represent points of engagement between the Web Services Division (the cloud service customer) and external stakeholders. The arrows represent the flow of information between external stakeholders and

the Web Services Division. Both the data flows and engagement mechanisms are influenced by how stakeholders are impacted by cloud services. A more detailed mapping of information flows should be undertaken to identify the exact information sources and destinations. While Figure 13 only illustrates specifics for external stakeholders, a similar exercise should be completed for internal stakeholders.

3. Identify stakeholder needs that result from the impacts defined in the previous step.

   Impacts are inextricably linked to needs. If there is a stakeholder impact, there is a stakeholder need. Even if a stakeholder's need is simple awareness or transparency, the cloud governance and management initiative is less likely to succeed if the CGMS does not address stakeholders' needs.

4. Categorize stakeholders. Use the categories below to associate a type with each stakeholder. This will help in prioritizing stakeholders. Each stakeholder is either A, B, or C.
   A. Primary – stakeholders who are directly impacted by cloud services.
   B. Secondary – stakeholders who are indirectly impacted by cloud services.
   C. Key – stakeholders for which buy-in for both cloud services and for the core tenets of the governance and management systems is a critical success factor for the initiative.

5. Prioritize stakeholders – key stakeholders should be given the highest priority, next primary, and then secondary.

Table 6 shows an example analysis of three stakeholders. Once you complete your stakeholder analysis it can be used as a baseline for further, downstream analysis. For example, a column could be added to the right of the 'Key Stakeholder Needs" column to define the corresponding cloud governance and management engagement strategy.

Stakeholders	Type	Impacts (on Cloud Services & Vice Versa)	Key Stakeholder Needs
VP of Web Services Division	Internal, Key	• Internal Senior Executive responsible for appropriate alignment of IT-related objectives and business • Responsible for the division's success and operational effectiveness	• Concise view of progress against objectives • Financial and technical performance of cloud services • Compliance status • Awareness of major issues and risks
Application Support Contractor	External, Primary	• Develop and support cloud-hosted applications. • Performs a major role in the end-user experience • Supports migration of applications • Must follow new and or revised application-related processes	• Awareness and training on new or modified policies, processes and procedures • Compatible development platform • Access to the cloud platform • Collaboration and coordination regarding cloud service transition and operations' activities
Cloud Service Provider	External, Primary	• Provider of cloud services • Interfaces directly with established processes • Provides monthly service reports	• Contractual, legislative, and regulatory requirements • SLA • Collaboration and coordination regarding cloud service transition and operations' activities

Table 6: Example of Stakeholder Analysis

Analyzed and Prioritized Cloud Service Objectives

The output of the effort described throughout this section is a rationalized list of prioritized cloud objectives. Based on the three previous tasks, you should have the following:

- Strategic cloud service objectives that were derived from strategic change drivers.
- Cloud service objectives that address operational change drivers.
- List of stakeholders and stakeholder needs.

Compile a single list by removing duplicates and creating a single list of unique measurable milestones. Use the SMART (Specific, Measurable, Achievable, Realistic, Time-phased) methodology to craft your objective statements. Once you have a working list of objectives, use a table similar to the one shown in Table 7 to analyze your objectives by assessing benefits, challenges, and risks associated with each objective. Table 7 contains examples of two cloud service objectives. The number of cloud service objectives an organization will have depends on the scope and size of the initiative.

ID	Operational Objective	Benefits	Challenges	Risk Considerations
1	Migrate Virginia corporate office to a cloud PaaS configuration by the end of 2015	• Compute and data resources available upon demand • Experienced and skilled PaaS staff maintains infrastructure and platform. • Decease in the number of performance-related incidents	• Proper planning and coordination between entities • Access and key management • Ensuring data security	• Transition is not appropriately planned and coordinated. • Access and keys are not appropriately managed. • Data is maintained in a jurisdiction with rules different from the US.
2	Transition and maintain corporate development environments to a cloud PaaS configuration by the end of 2015.	Consolidated management and maintenance of all environments (e.g., development, staging, production, and warm standby) resulting in a reduction in overall development costs.	• Proper planning and coordination between entities • Access and key management	• Transition is not appropriately planned and coordinated. • Access and keys are not appropriately managed.

Table 7: Example Cloud Service Objectives and Supporting Analysis

Chapter 8: Step 4-Integrated Cloud Governance & Management System

Once objectives are determined, analyzed, and prioritized the next step is to define an integrated CGMS that is consistent with cloud service principles and enables the realization of cloud objectives. Many organizations may already have an IT governance and management capability. In such cases, the contents of this chapter should provide some insight regarding how to adapt your current capability to better support cloud services.

The components of the CGMS are listed below:

- Principles – principles provide a succinct interpretation of desired organizational behavior and present them in a set of guidelines for day-to-day activities and decisions. Principles also provide guidelines for the development and execution of policies and other system components. (Defined in Chapter 6)
- Reference Model, Policies, Processes, Procedures, and Tools– the reference model provides, in a snapshot, the interrelated processes, tools and other components of the CGMS. Policies, processes, procedures, and tools will be consistent with the reference model.
- Cloud Governance and Management Organizational Structure – the governance and management organizational structure is the visual representation of the organization that is responsible for using the system to realize cloud service objectives.
- Roles and Responsibilities – roles and responsibilities define who is responsible for performing which governance and management functions.
- Communication and Reporting – communication and reporting represent the CGMS stakeholder engagement requirements and corresponding information flows.
- Training and Education – training and education are cornerstones to an effective, sustained governance and management capability. This component of the CGMS defines training and education needs and methods.

The following sections detail how to define each of the listed CGMS components.

Reference Model, Policies, Processes, Procedures, and Tools

Cloud governance and management are process-based activities. To develop a reference model you have to identify which processes your organization will use for both cloud governance and cloud management. Following is a list of governance and management process-related guidelines to help you establish a process architecture for your CGMS.

Cloud Governance Processes

As we discussed in Chapter 2, for IT governance, there are two widely accepted standards or frameworks, COBIT 5 and ISO/IEC 38500. The COBIT 5 framework defines 37 non-prescriptive processes that fall into one of five governance and management domains—(1) Evaluate, Direct and Monitor; (2) Align, Plan and Organize; (3) Build, Acquire and Implement; (4) Deliver, Service and Support; and, (5) Monitor, and Evaluate and Assess. The governance domain, Evaluate, Direct and Monitor, contains the following five processes:

- Ensure Governance Framework Setting and Maintenance
- Ensure Benefits Delivery
- Ensure Risk Optimization
- Ensure Resource Optimization
- Ensure Stakeholder Transparency

The remaining 32 processes fall within the remaining four IT management domains.

For each of the five processes in the COBIT 5 governance domain there are associated activities. The activities fall into one of the three governance categories—Evaluate, Direct, or Monitor. For example, the process "Ensure Benefits Delivery" has a set of Evaluate activities, a set of Direct activities, and a set of Monitor activities. The COBIT 5 framework is extensive, and is defined in several documents. The framework was developed to support enterprise-level IT governance.

ISO 38500 is an international standard that is exclusive to IT governance. Unlike COBIT 5, which is a

framework and addresses both IT governance and IT management. In ISO 38500 processes are not defined, instead there are six principles—Responsibility, Strategy, Acquisition, Performance, Conformance, and Human Behavior (ISO & IEC, 2008, p. 6). Similar to COBIT 5 and its processes, each principle has associated with it activities that fit into each one of three categories—Evaluate, Direct, and Monitor. The ISO 38500:2008 standard is a 15-page document that is used primarily as a principle-centered framework for IT governance. The publisher has recently released a 2015 version of ISO 38500.

The approach we will take leverages both the ISO 38500 and COBIT 5 approaches by defining activities within the context of Evaluate, Direct, and Monitor, associating activities with principles, and associating activities and principles with processes. For example, if there is a principle titled “Alignment”. It may have a process titled “Alignment of Cloud Services with Business and IT." The process in turn will have associated activities within each governance category (i.e., Evaluate, Direct, and Monitor).

For each of your organization’s cloud service principles defined in Chapter 6, characterize a corresponding governance process. The process, and the name of the process, should embody what is necessary to manifest the principle fully. 8 provides an example of defining processes that correspond to principles.

As you define the processes that best correspond to your organization’s cloud service principles, recall the definition of cloud governance from Chapter 2, "Cloud governance is the subset of IT governance that embodies the tools, and capabilities needed to establish the organizational direction for cloud computing consistent with business and stakeholders’ needs, and to ensure the direction is followed in a manner that minimizes risks and optimizes value to the organization.

In addition, when defining processes, consider the COBIT 5 processes as best practices. However, the COBIT 5 processes should be tailored and augmented to accommodate cloud service considerations and the specific needs of your organization. Both principles and processes should minimally address the following core tenets of IT governance and cloud computing-related considerations:

- Strategic Alignment
- Value Creation
- Stakeholder Management
- Risk Management
- Performance Management
- Compliance
- Security
- Process Agility

The names of the processes should correspond to both the principle and to the activities that will support it.

With processes defined, now we can define the corresponding activities associated with Evaluate, Direct, and Monitor. Essentially we are defining what has to be evaluated, directed, and monitored to ensure the principle is upheld and the purpose of the process is being met. One process may address multiple principles. For example, the two principles Responsibility and Accountability could both be addressed in a single process “Assign Responsibility and Manage Accountability”.

Table 9 is an example mapping of principles, processes, and governance activities. This task is best completed by the CPIT with input and buy-in from the E-CPIT.

Cloud Governance Principles	Cloud Governance Processes	Entrance Criteria	Exit Criteria	Purpose
Alignment	Alignment of Cloud Services with Business and IT	Business and IT strategic goals and objectives are aligned.	Cloud service objectives have been aligned, defined, and realized.	The purpose of this process is to define cloud service objectives and to ensure that they are met. Cloud service objectives should appropriately support the accomplishment of business and IT strategic goals and objectives and address stakeholder needs.
Responsibility	Assign and Manage Responsibilities	CGMS processes and Activities have been defined.	CGMS roles, responsibilities, and corresponding competencies are defined and successfully executed.	The purpose of this process is to ensure that roles, responsibilities, and corresponding competencies for the CGMS are appropriately defined and implemented.

Table 8: Example of Governance Principles and Corresponding Processes

Cloud Governance Principles	Cloud Governance Processes	Cloud Service Governance Activities		
		Evaluate…	Direct…	Monitor…
Alignment	Alignment of Cloud Services with Business and IT	• To ensure cloud service objectives align with business and IT strategic objectives and stakeholder needs. • Plans, policies, and cloud service activities to ensure they align with the organization's cloud service principles and objectives. • Internal and external change drivers and ensure their consideration in objectives, plans and policies.	• That the preparation and use of plans and policies align with cloud service principles and objectives. • The assignment of CGMS responsibilities.	• Progress of improved cloud service capabilities against proposals to ensure that they are achieving objectives in required timeframes using allocated resources. • Use of cloud services to ensure achievement of intended benefits.
Responsibility	Assign and Manage Responsibilities	• Responsibilities and associated competency requirements for cloud service-related decision making. • Assignments to ensure roles and responsibilities are assigned, and that competencies and roles are appropriately matched.	• The execution of plans ensuring that they are carried out according to assigned cloud service responsibilities. • That stakeholders receive the information that they need to meet their responsibilities.	• The establishment and appropriateness of cloud governance mechanisms. • Acceptance and understanding of assigned responsibilities. • The performance of those given responsibility in the governance and management of cloud services.

Table 9: Example Governance Mapping

Once you have defined processes and activities for each principle, and both the CPIT and E-CPIT are in agreement, the processes have to be documented, and policies have to be developed that address the processes. See the Policies and Procedures section in this chapter for more on policies.

Cloud Management Processes

There are a number of widely accepted standards and frameworks that address ITSM in whole or in part, including COBIT 5, CMMI-SVC, ITIL, ISO 9001, ISO/IEC 20000, and ISO 27001. Standards bodies and similar

organizations with some of the smartest people in the universe expend significant resources and invest years to define and refine IT management processes. There is no need to reinvent the wheel. To define the cloud management processes that will support the accomplishment of your organization's cloud objectives, map your objectives against the industry recognized standards and frameworks that will best meet your needs. Figure 14 provides an example of the mapping of cloud objectives to ITIL Service Transition and Service Operations processes. Check marks are used in Figure 14 to show those processes affected and/or needed to implement the objectives. The example shown in Figure 14, only illustrates mapping against two ITIL life cycle components, Service Transition and Service Operation. It is important that your actual mapping occurs against an entire life cycle to make sure all aspects of the cloud service objective's implementation are considered.

	Cloud Service Objectives			
	Acquire, Implement & Maintain PaaS	Transition & Maintain Dev. Environ	Transition & Maintain XYZ App.	Transition & Maintain Warm Standby
Service Transition				
Transition Planning & Support	√	√	√	√
Change Management	√	√	√	√
Service Asset & Configuration Management	√	√	√	√
Release and Deployment Management	√	√	√	√
Service Validation & Testing	√	√	√	√
Evaluation	√	√	√	√
Knowledge Management	√	√	√	√
Service Operation				
Service Desk	√		√	
Event Management	√			
Incident Management	√	√	√	√
Request Fulfillment	√	√	√	
Problem Management	√	√	√	
Access Management	√	√	√	√
IT Operations Management	√	√	√	√
Apllications Management			√	√
Technical Management	√	√	√	√

Italics indicate functions or roles.

Figure 14: Example of Objective Mapping

Before you select the management processes against which you will map your organization's cloud service objectives, consider the following six important points:

1. If your organization already has an ITSM capability, this exercise should help you examine which components of your existing process architecture to tailor or amend to best support cloud computing, or which process areas should be added. You should begin by mapping your cloud service objectives against the ITSM system you currently have in place to identify which processes are impacted by each cloud service objective. Then you should identify the gaps in those processes between what is needed to support cloud services and what already exist. Next modify those processes to fill the gaps. The CPIT should manage both the mapping process and the modification or addition of processes. Following is a list of some key impacts cloud services will likely have on existing ITSM processes:
   - o Service Strategy
   - o Strategy Generation – as applicable, defining brokerage strategy, partners, and value that will meet customer needs.

- Financial Management – budgeting and accounting for metered services (cloud services) and chargebacks associated with missed SLA targets.
- Demand Management– Defining and managing service consumption activities that will impact costs.
- Service Design
- Service Catalog Management – establishment, maintenance, and communication of the service catalog.
- Service Level Management – defining appropriate service level targets, ensuring the suitable negotiating, measuring, monitoring and reporting associated with SLAs and OLAs.
- Capacity Management – assessing the capacity needs of the organization, the better the sizing the more accurate the budgeting process as well as the pricing in some broker configurations.
- Security Management – appropriate controls and monitoring to ensure confidentiality, integrity and availability of data located in the cloud; monitoring the service provider's compliance with regulatory and contract security requirements; consideration of data sensitivity in multi-tenant configurations.
- Service Continuity Management – coordination with the cloud service provider on the disaster recovery plan; as appropriate updating the disaster recovery plan to include components located in the cloud and adequately communicating the updated plan with all affected stakeholders.
- Service Transition
- Transition Planning & Support – coordination between IT, service provider(s) and application team(s); establishment of a common language between entities; integrated schedules and activities.
- Change Management – more agile processes to support accelerated implementation timelines, increased coordination and collaboration on changes and change windows (e.g., development, service provider, IT, end users, etc.).
- Asset & Configuration Management – fewer physical assets to manage and more logical assets to track and manage.
- Release and Deployment Management – need for platform/capability to support coordination and communication between service providers, application development teams, and relevant stakeholders regarding releases, patches, and other such system updates.
- Service Validation & Testing – a migration plan that defines roles and responsibilities of the service provider, application team, and existing infrastructure team to support the migration of applications to the cloud; coordination between relevant stakeholders to migrate applications.
- Service Operation
- Incident & Problem Management – need for capability to manage and coordinate incidents and problems across service provider (s), application team (s), IT, and other relevant stakeholders; sharing of known issues, workarounds and other such information.
- Event Management – ensure the appropriate monitoring and event response coordination across relevant stakeholders.
- Access Management – accommodating user profiles and authentication information located outside of the cloud service, including connectivity and a need for periodic reconciliation; controls that account for multi-tenant environments; as appropriate, control of the development environment; identity management that supports users acting on their own behalf or on behalf of an organization; as appropriate, support for single sign-on capabilities.
- Request Fulfillment – ability to communicate, coordinate, track, and manage service requests.

2. If your organization does not currently have a service management capability, start with ISO/IEC 20000 processes and fill the gaps with ITIL processes. The ISO/IEC 20000 is an international standard based on portions of ITIL that defines specific requirements for establishing a service management system. Standards are typically easier to get your arms around since they have very specific requirements. The ITIL is a comprehensive library of service management processes and related details that emphasize the "how". Since cloud computing is an IT service, these standards and best practices are a logical starting point. How the processes, ITIL in particular, are actually implemented will require some specific accommodations for both cloud computing and your organization's dynamics and structure.

Other standards and best practices may also be used to augment ISO/IEC 20000. For example, neither ISO/IEC 20000 nor ITIL thoroughly addresses risk management. Therefore, an organization may choose to integrate the risk-management process from CMMI or the ISO 31000 risk management standard.

3. Appropriately select standards and best practices that address all aspects of your organization's service management needs, to include compliance and risk management. There is a likelihood that you will use more than one industry standard or framework to address your needs fully. For example, because of the CMMI-SVC expertise and process architecture within your organization, you may decide to use CMMI-SVC as the primary framework and fill any gaps with ITIL processes. Table 10, presents a summarized description of key advantages and disadvantages of a few industry-recognized ITSM full-life cycle-management standards and best practices.

Standards/Best Practice	Key Advantages	Key Disadvantages
ITIL	• Addresses comprehensive service lifecycle management • Extensive content for each process area that emphasizes the "how". • Widely accepted international best practice.	• Does not directly address compliance or risk management and will require the use of other process areas outside of ITIL to address these areas. • Even though the price has declined over the years, the full set of ITIL books still cost approximately $500. • Does not contain specific requirements, instead provides detailed descriptions of process area.
ISO/IEC 20000	• An international standard with very specific compliance requirements. • Contains internal audit requirements that can be leveraged to address compliance. • Emphasizes the "how". • Based on ITIL and ISO 27001.	• Does not directly address risk management. • Does not directly address some of the ITIL processes that are advantageous in cloud implementations (e.g., demand management, strategy generation, etc.).
COBIT 5	• Addresses risk management and compliance • Large breath of content that covers both management and governance and emphasizes the "what". • Holistic, beginning with alignment between IT objectives, business objectives and stakeholder needs.	• Has high-level processes without technical details. • Emphasizes the "what" not the "how". • Will likely require the use of other processes and frameworks to address the "how".
CMMI-SVC	• Addresses risk management and can accommodate compliance. • Comprehensive service management framework with emphasis on the "what" and specific examples of "how". • Embedded maturity levels and high-level implementation road map (i.e., staged implementation).	• Not specific to technical services. • Does not address demand management, financial management and other strategy-related process areas.

Table 10: Comparison of ITSM Full Lifecycle Standards and Best Practices

4. Defining which combination of industry standards and best practices to use within an organization is best accomplished by someone knowledgeable about and experienced with implementing ITSM processes. If no one in your organization has the appropriate skill set, you should seek the support of a consultant. Your organization should also provide or acquire formal training for personnel responsible for implementing and maintaining processes.
5. There is significant overlap between many of the ITSM standards and frameworks. With varying levels of detail, many of the management standards and frameworks address some of the same process areas. There are other standards that are particular to a single process area with minimal overlap. For example, ISO 27001 is specific to Information Security Management, but has some overlap with some of the other ISO standards.
6. Depending on the scope of your cloud services' initiative, there may be roles your organization may need to fill before and after cloud services are implemented. Roles that may not exist prior to implementing cloud services. Depending on the cloud services' strategy, one or more of the following roles will likely need to be filled by your organization:
    - **Service Provider** – Responsible for communicating, supporting, and providing cloud services to internal or external customers. These are services acquired from a CSP to host organizational applications, or services acquired to provide cloud-based applications (e.g., Salesforce.com, MS Office 365, etc.) to internal customers. This role would also be responsible for managing application-level access to cloud services.
    - **Service Integrator** – Responsible for ensuring the appropriate coordination and communication between CSPs and internal and external service partners. This role is particularly important in a multisource environment in which multiple external suppliers are involved in the delivery of services. The Service Integration and Management (SIAM) framework may be useful in multisource environments. The main goal of SIAM is to coordinate internal and external suppliers and their services to achieve the end-to-end service levels needed to support business needs. SIAM implementations encounter significant challenges and should be well considered before implementation.
    - **Service Consumer** – the recipient of cloud services that has a business relationship with the CSP. The Service Consumer is responsible for tracking and managing service levels, ensuring compliance with information security and other requirements. As appropriate, this role would also be accountable for managing administrative access and access to the application development environment.
    - **Service Broker** – Responsible for providing value-based hosting services to other business units or groups within the organization.

As with governance processes, for each process or group of processes policies are developed and agreed to by the CPIT and E-CPIT.

Policies and Procedures

Similar to principles, policies establish a behavior or performance expectation, but are more specific than principles. For example, an "Agile Processes" principle may generally dictate streamlined processes. A corresponding policy may indicate that peer reviews are required for non-major changes, but approvals are not required. Policies may also dictate the use of a specific standard or framework such as ITIL, CMMI-SVC or ISO 27001. The E-CPIT is responsible for developing or approving policies.

To recap, principles will typically have associated processes, and processes will typically have associated policies and procedures. However, there is not necessarily a one-to-one relationship between processes and policies. An organization could decide to adopt a standard and/or framework as a general policy that addresses all or most of the processes. Some organizations with defined principles opt not to have policies at all. I would caution against a principle-only approach. While an organization may not want to introduce burdening policies and procedures, too much flexibility can yield unpredictable and unmanageable outcomes. The CPIT should maintain a portfolio of policies and ensure they are agreed to by the E-CPIT, managed, and continually improved. As with principles, volatility with organizational policies will diminish their credibility and effectiveness.

Ultimately, procedures have to be defined that provide the "how" for the processes, in a manner that is

consistent with policies. Processes can't be effectively communicated and followed unless they are documented with associated procedures and activities that describe the "how". For small organizations, in particular, procedures should be light, simple, and flexible.

The more detailed and comprehensive the procedure, typically the greater the cost to both execute and maintain it. When documenting procedures it is important to strike the right balance between effectiveness and cost. To keep procedures light and simple use flow charts and/or checklist instead of wordy documents to communicate the procedure. Layer procedures to ease navigation and make sure each step has supporting rational. Develop templates to ensure CGMS artifacts have all of the required elements and that procedures are repeatable. When processes and procedures are documented inputs, outputs, and decision points should be clearly identified. I have used these procedure-documentation techniques more times than I can count. By far, procedures documented in this manner are easier to follow, simpler to manage, and are more sustainable. While those closest to procedures should be involved in their development, all procedures should be approved for use by the CPIT.

Tools

Identifying, acquiring, and adopting tools is extremely helpful in standardizing how policies, processes, and procedures are executed. An organization can ensure a process is being followed by mandating the use of a carefully selected tool. The tool in turn enforces the desired policies and procedures. For example, your organization can require that all risks have an associated rating. Mandating the use of a risk-management tool that automatically calculates a risk rating based on inputs such as impact and likelihood, creates consistency and standardization. In most instances, processes should be automated to the maximum extent possible.

One of the challenges with cloud services is that someone else is managing the environment, often making it difficult to get verifiable, quantitative performance data. Automated tools such as PerfKitBenchmarker and PerfKitExplorer allow you to get a transparent view of application throughput, latency, variance, and overhead associated with cloud services. It then visualizes the data is colorful dashboards. Performance tools can also assist in assessing performance against SLA targets and in estimating how applications may behave in advance of migration.

In many instances, automated tools are nice-to-haves with a substantial value proposition. In other instances, tools are mandatory for an effective CGMS. Tools such as ticketing systems to track and manage service requests and incidents, content management systems to store and make accessible processes and procedures, and collaboration tools to coordinate schedules and other shared information with CSPs and internal stakeholders.

Network and system monitoring tools are also critical, but are primarily the responsibility of the CSP. Organizations should assess the automated management (e.g., patch management, event management, etc.), monitoring, and reporting capabilities of CSPs during the acquisition process.

To define opportunities for tool adoption within your organization's CGMS, list all the governance and management processes and corresponding process steps your organization will use, then identify those activities that can be automated. Since most organizations can't automate all processes, start with coordination and collaboration processes and customer facing processes such as incident and service request management, and automate other processes when possible.

Cloud Governance and Management Reference Model

Now that we have defined the CGMS principles, management and governance processes, and tools, we can create a graphical reference model that illustrates, in a snapshot, an integrated cloud governance and management model. Figure 15 depicts an example of an integrated cloud governance and management reference model. The reference model should foster understanding of the CGMS and facilitate the use of a common CGMS language.

You should be as specific as practical with your reference model and include components such as tools, relationships, processes, and information flows.

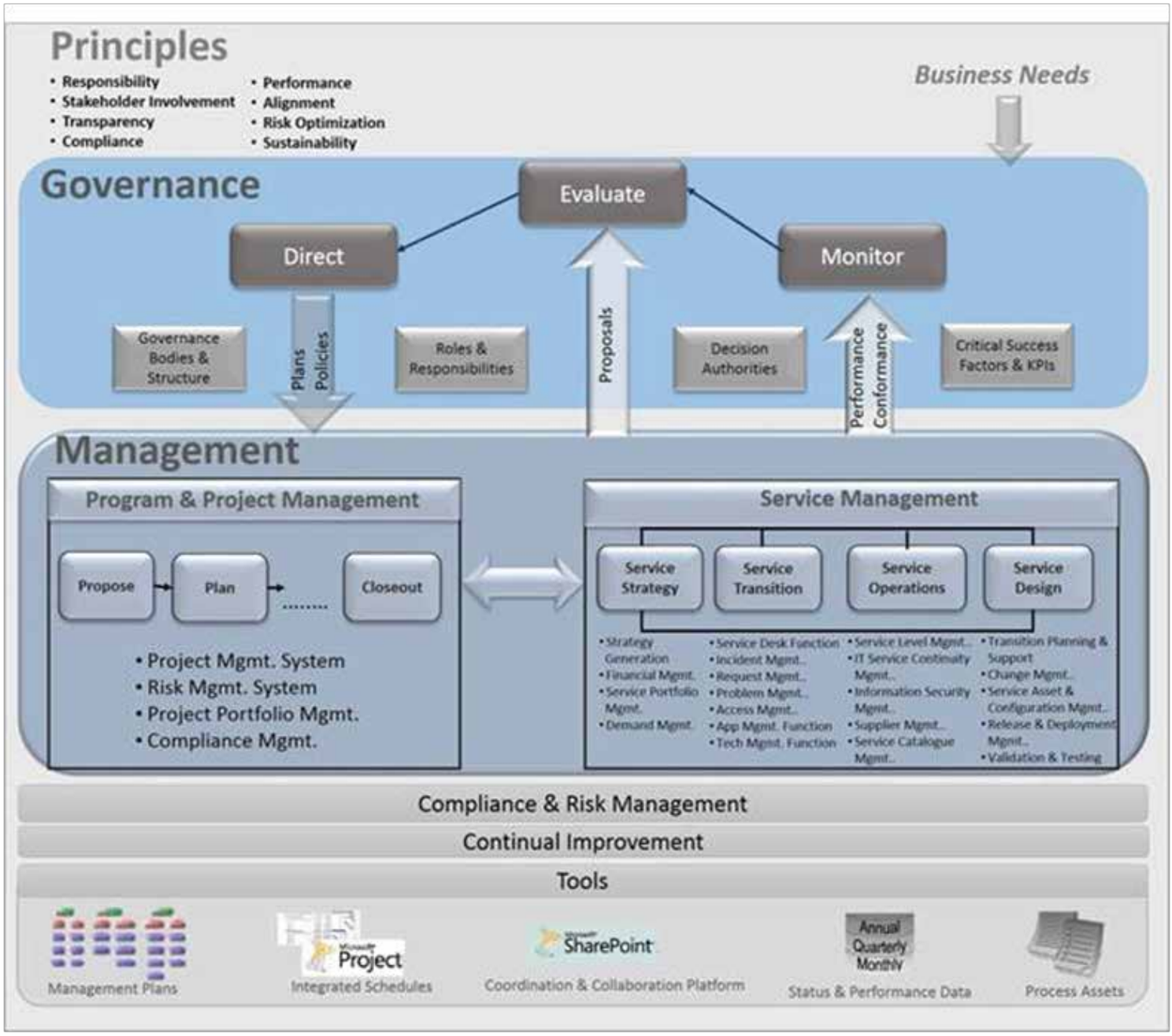


Figure 15: Example Integrated Cloud Governance and Management Reference Model Organizational Structure and Roles and Responsibilities

Cloud Governance and Management Organizational Structure

The CGMS organizational structure provides context and definition to the team of individuals who will operate within the reference model shown in Figure 15. Organizational structure provides context for roles and responsibilities and how they are assigned, coordinated, and managed. The CGMS organizational structure will depend on an organization's objectives and strategy for cloud governance and management. Similar to the CGMS implementation team (i.e., CPIT, E-CPIT, etc.), the goal for the CGMS organization is for it to have the appropriate business and IT cross-functional stakeholder representation, to include engaging each management tier. Figure 16 is an example of a CGMS organizational structure. The diagram shows a fictitious organization with a governance and management body that consists of an Executive Cloud Governance Board, a Cloud Governance Committee, and a Cloud Management Working Group. The roles and responsibilities associated with each group are described in Table 11.

The task of defining your organization's governance and management organizational structure is best completed by the CPIT and finalized by the E-CPIT. Following are some general guidelines for designing your organization's governance and management structure:

1. Review and understand the goals and strategies for the CGMS, and design an organization that enables and supports the vision for the CGMS.
2. Review and understand the enterprise-cloud-service strategy, and ensure the CGMS organization is appropriately aligned.
3. Ensure representation from both business and IT executive leadership.
4. Implement a hierarchical structure that focuses executive participation on strategy development and clarification, defining and managing principles, risk management, policy review and approval, and financial decisions.
5. Ensure key stakeholders are adequately represented and/or involved throughout the life cycle of the CGMS.
6. As appropriate, include a cross-section of stakeholder representation at each level.
7. Include practitioners in the development and review of processes and procedures.
8. Establish governance domains that arrange processes based on life cycle phases or similar grouping.
9. Transparently communicate with the organization throughout the process.

The Executive Cloud Governance Board should ensure a clear charter exists for the cloud governance and management organization. The charter should minimally address the purpose behind the organization, its goals and objectives, meeting and reporting requirements and formats, and roles and responsibilities.

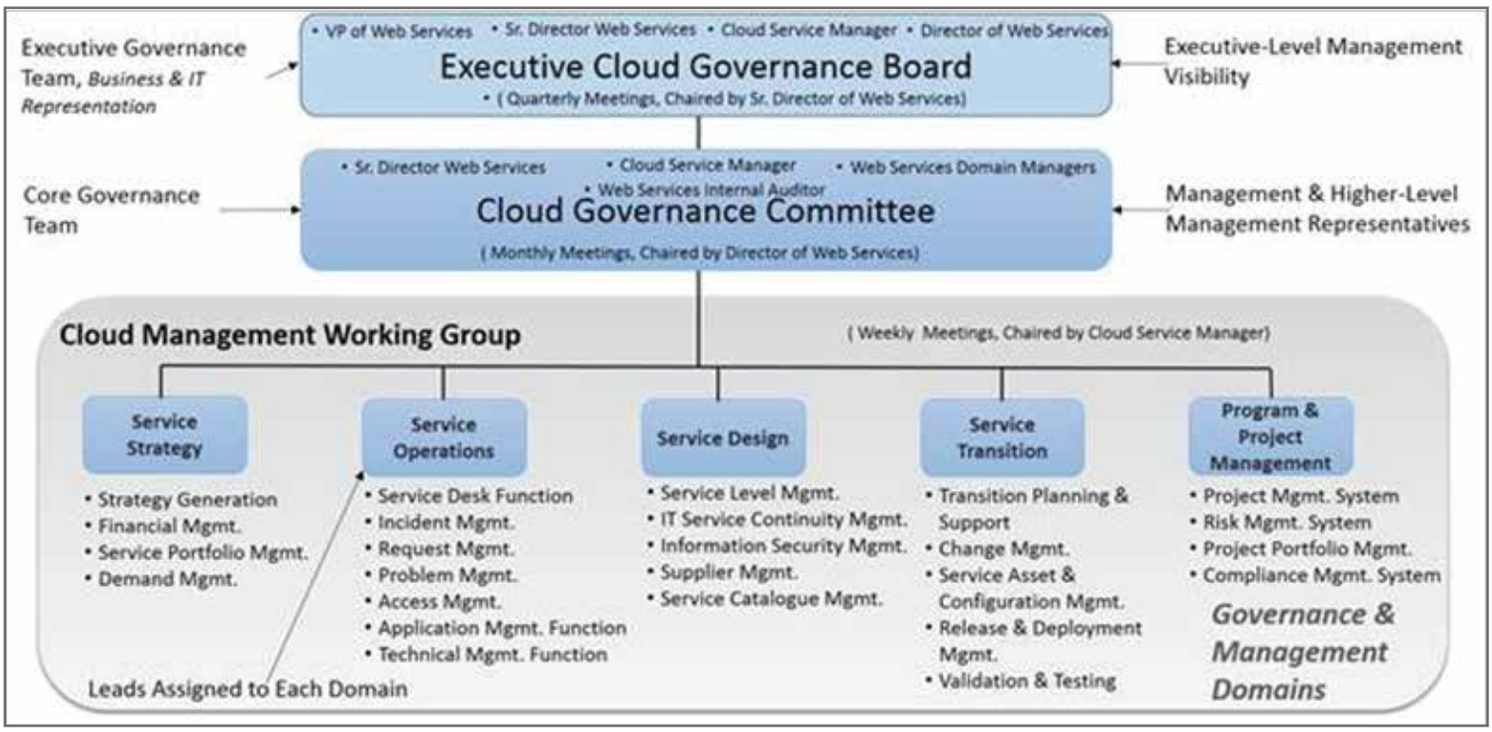


Figure 16: Example of a Cloud Governance and Management Organizational Structure

Roles and Responsibilities

Figure 16 shows the fictitious Web Services Program's governance and management organization. In addition to the working bodies (i.e., Executive Cloud Governance Board, Cloud Governance Committee, Cloud Management Working Group), there are individual roles that can be added to the diagram based on the planned or existing ITSM organization.

Individual roles are necessary for the CGMS to function and are defined based on the needs and structure of an organization. Individual roles in the example CGMS organization shown in Figure 16, would likely include a

Chair for each entity (i.e., Board Chair, Working Group Chair, Committee Chair, etc.) and Domain Managers/Leads for each governance and management domain (e.g., Service Strategy, Service Operations, Service Design, etc.). Roles and responsibilities should be defined for each group or individual who is a member of the CGMS. Table 11 provides an example of CGMS roles and responsibilities that correspond to Figure 16.

CGMS Roles	CGMS Responsibilities
Executive Cloud Governance Board	This role evaluates, directs, and monitors, alignment of cloud service objectives with business and IT objectives, policies and principles, performance against cloud service objectives, performance against service-level targets, performance against budget, major changes and improvements, major issues and risks, and status of benefits realization.
Cloud Governance Committee	This role ensures alignment of activities with cloud service objectives, alignment of processes and procedures with policies and principles, risk and compliance management activities are executed, performance against plans, performance against targets and other requirements (e.g., legislation, regulations, contractual requirements, etc.); changes and improvements are identified and appropriately managed; serious identified and appropriately managed, and benefits are realized.
Cloud Management Working Group	This group plans, implements, manages and improves cloud services process assets and related projects. It ensures activities adhere to established processes and procedures, ensure appropriateness of processes and procedures, and performance against objectives and budget.
Committee/Group Chair	These individuals, or their designees, are responsible for facilitating meetings consistent with the charter, preparing agendas and presentations, establishing a communication's plan for the group that is consistent with the charter, ensuring Task Forces or working groups are appropriately established and managed (e.g., objectives, tasks, timelines, etc.), documenting meeting minutes, and for tracking action items to closure.
Domain Manager/Lead	These individuals ensure processes and procedures are documented, and along with tools, are consistent with policies and principles. These individuals also assign process owners, ensure the coordination of processes within and across domains, approve processes and procedures within their domain, and represent process owners in Cloud Management Working Group meetings.

Table 11: Example of CGMS Roles and Responsibilities

It is noteworthy that an individual or group can perform multiple roles, depending on the size and needs within the organization.

Decision Framework

According to the Weill and Ross Research (2004), organizations with clarity and focus gained above-industry-average value from IT. A large part of that clarity is understanding what types of decisions must be made and assigning responsibility for those decisions. In IT governance: How Top Performers Manage IT Decision Rights for Superior Results, (Weill & Ross, 2004) six IT-related decision types are defined. These six decision types were used as input to determine the following set of cloud decision types:

- Cloud Principle Decisions – cloud principles are high-level statements about how cloud services will be used within the organization.
- Cloud Architecture Decisions – cloud architecture relates to enterprise-level standardization and

integration guidance (e.g., policies, technical alternatives and choice, etc.) associated with the rationality of data, applications, and infrastructure.

- Cloud Infrastructure Decisions –cloud infrastructurerelates to shared and coordinated (organization or enterprise-level) foundational approaches to the configuration of cloud service delivery and support.
- Cloud Business Application Needs Decisions – cloud business application needs relate to business needs for applications hosted in the cloud.
- Cloud Investment and PrioritizationDecisions – cloud investment and prioritization relate to the need for, and the cost and priority of cloud and related services used to meet specific business needs.

For each decision type, Table 12 defines an example of who will make which decisions and who will provide input. Generally, decisions should be made by the manager closest to a situation. When developing a decision framework for your organization, consider the business goals and strategies and define the Decision Framework accordingly. For example, an organization that is implementing a cost-reduction strategy would likely have cost-related decisions made centrally. An organization implementing a customer-excellence strategy may have related decisions made as close to the customer as possible.

The "Input" column in Table 12 defines which organizations or individuals will provide input to the decision process, and the "Decision" column identifies which group or organization will make the decision. Establishing decision rights is important because it can help ensure the appropriate consideration goes into cloud-related decisions. However, for a decision framework to be effective, it has to be communicated and understood by the organization. Training on the CGMS should be required for everyone within the organization.

Decision Types	Inputs	Decisions
Cloud Service Principles	• Cloud Governance Committee • Cloud Management Working Group	Executive Cloud Governance Board
Cloud Architecture & Infrastructure	• Cloud Management Working Group • Enterprise Architecture Group • IT Manager	Cloud Architecture Sub Committee
Cloud Business Application Needs	• Users	Business Managers
Cloud Investment & Prioritization	• Business Manager • Service Manager	Executive Cloud Governance Board

Table 12: Examples of Decision Authorities

Communication & Reporting Requirements

Communication is the oil for the CGMS engine. Without the appropriate communication, the CGMS will become ineffective and a source of frustration for the organization. Communication and reporting should always be a part of any planning process, and the CGMS is no exception.

To define communication and reporting requirements, start with a comprehensive list of cloud service stakeholders (see Stakeholder Analysis in Chapter 7). Using the previous stakeholder analysis as input, for each stakeholder define the flow of information into and out of the CGMS. As a result of the information flows, the type of stakeholder (i.e., key, primary, secondary, etc.), and impacts and stakeholder requirements, define the stakeholder communication and reporting requirements. Table 13 provides an example of information flows into and from the CGMS and corresponding communication and reporting requirements.

Stakeholders	Data Flow Into CGMS from Stakeholders	Data Flow Out of CGMS to Stakeholder	Reports Out of CGMS to Stakeholders
Enterprise-Level Senior Executives	Strategic Direction	• Upon Request – Responses to Questions and Briefings	None
Organization-Level Business Executives	• Strategic Objectives • Feedback resulting from quarterly briefings • Feedback Resulting from adhoc requests • Judgment and direction	• Upon Request – Responses to Questions and Briefings • Recurring Cloud Service performance reports/briefing	Quarterly cloud governance Briefing – New Policies, Changes to existing policies, serious risks and statuses, planned improvements, compliance, serious issues and their statuses, performance against objectives and critical success factors, and status of benefits realization.
Organization-Level IT Executives	• Strategic Objectives • Feedback resulting from quarterly briefings • Feedback Resulting from adhoc requests • Judgment and direction	• Upon Request – Responses to Questions, Briefings • Recurring Cloud Service performance reports/briefing	Quarterly cloud governance Briefing – new policies, changes to existing policies, serious risks and statuses, planned improvements, compliance status, security status, serious issues and their statuses, performance against objectives and critical success factors, and status of benefits realization.
Enterprise Architecture Group	Decisions and Guidance	• Requests for guidance and/or approval consistent with rules established by Architecture Board and other enterprise-level IT governance entities.	None

Table 13: Example of Communications & Reporting Requirements

Chapter 9: Step 5-Implement & Institutionalize

Implement

Now that we have discussed how to develop the core components of the CGMS, with both understanding and context, we can discuss implementation. Figure 17 summarizes the steps presented throughout this plan along with the outputs produced at each step. Following is a list of key points to recall as you plan and implement your organization's CGMS:

- **Preparation and Planning** – an executive sponsor, implementation-team lead, and cross-functional implementation team are needed to plan, design, implement, manage, and continually improve the CGMS. The team should consist of the appropriate mix of IT and business stakeholders to include executives, managers, and practitioners. The team should have a formal charter and be educated on its contents. Once the team is established and trained, the next order of business is to develop a plan and schedule for the CGMS initiative. The business case is used as input to the planning process. Among other things, the plan should include a team communication framework, schedule, clearly defined objectives and milestones that are approved by the team, and Critical Success Factors (CSFs) for the initiative. The CGMS initiative is planned like a service and not a project; a service that has to be maintained and continually improved. Risks to the success of the CGMS implementation and issues associated with implementation are tracked and managed by the implementation team.
- **Guiding Principles** – appropriately defined cloud service principles are critical to the success of the CGMS. Principles establish guidelines for the desired character, effectiveness, and performance of the CGMS. The goal of cloud service principles is to affect the behavior of the organization, such that business goals are met; the organization's values are upheld, and the mission of the organization is furthered. Cloud service principles will influence day-to-day decisions related to cloud services and requirements for CGMS components such as polices, processes, and tools.
- **Alignment Framework & Cloud Service Objectives** – the alignment framework defines the approach used to craft cloud service objectives that align with business and IT strategic and operational objectives. Strategic and operational change drivers and stakeholder needs are used to define cloud service objectives. Cloud service objectives are defined using the SMART (Specific, Measurable, Achievable, Realistic, Time-phased) methodology. For each objective, corresponding benefits and risks are defined, tracked, and managed through closure. Defining and managing objectives are continuous processes.
- **Integrated Cloud Governance and Management System** – an integrated CGMS minimally consists of the governance and management process architectures, governance and management organization structure, roles and responsibilities, the decision framework, and reporting and communication requirements. The CGMS is managed and maintained by the CPIT.
- **Implementation and Institutionalization** – implementation and institutionalization consists of documenting and managing changes to the process infrastructure, training the organization on any process infrastructure revisions, defining critical success factors and corresponding key performance indicators, and continually identifying improvement opportunities as well as correctives and preventative actions and tracking them to closure. Frequent and rigorous process and service assessments should be conducted, and corrective actions tracked to closure. More frequent assessments can accelerate the implementation of the CGMS.

An important implementation consideration is the size appropriateness of policies, processes and procedures. Size appropriateness is typically characterized by the depth and breadth of the processes and procedures compared to an organization's available resources. The more extensive the processes and procedures the greater the process overhead and the greater the resources required to manage and maintain them. The use of automated processes, checklists, and templates can streamline the process and procedure definition process, as well as limit process execution times.

If your organization is implementing a new governance and management capability, it may be helpful to develop process and procedure templates that your team can use to document your processes and procedures. The templates will ensure consistency in the way information is presented and activities are defined.

Figure 17: CGMS Implementation Roadmap

Implementation of the CGMS should be done in phases with timetables and deliverables. Implementation may require cultural change and transformation for which organizational change management techniques would be beneficial.

CGMS Process Maturity

Maturity of the CGMS is characterized by increases in the sophistication and performance of its processes. Achieving these increases in performance and sophistication is a continual process that is executed through a series of incremental improvements accomplished over time.

The COBIT 5 product set includes the following process capability model, based on the internationally recognized ISO/IEC 15504 Software Engineering—Process Assessment standard and the CMMI capability maturity model (ISACA, 2012, p. 44):

- **Level 0**: Incomplete Process - The process is not implemented or fails to achieve its purpose.
- **Level 1**: Performed Process - The implemented process achieves its process purpose.
- **Level 2**: Managed Process - The level one performed process is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.
- **Level 3**: Established Process - The level two managed process is now implemented using a defined process that is capable of achieving its process outcomes.
- **Level 4**: Predictable Process - The level three established process now operates within defined limits to achieve its process outcomes.
- **Level 5**: Optimizing Process - The level four predictable process is continuously improved to meet relevant current and projected business goals.

The CGMS will mature as a result of its processes (e.g., information security, alignment, incident management, etc.) maturing over time through structured and continual improvements. The CGMS improvements should be managed and implemented by the CPIT.

CGMS Initiative Critical Success Factors

Critical success factors define key areas of performance that are essential for the organization to accomplish its mission (Caralli, 2004, p. 2). The CGMS initiative's CSFs define key areas of performance that are vital to the successful implementation of the CGMS. While CSFs are discussed here, in Chapter 9 of this plan, they should be defined during the planning process so that CSF-related activities can receive management attention throughout the CGMS's implementation. Critical success factors, their associated measures, and supporting narrative should be reported to the CPIT and E-CPIT on a routine and event-driven basis to ensure the initiative stays on track. Typically, CSFs are not quantitative. As such, a mechanism is needed to measure the performance of CSFs and assess the health of the CGMS implementation. Table 14, lists some example CSFs for a likely CGMS implementation. As shown, Key Performance Indicators (KPIs) are used to quantify CSFs.

A KPI is a measurement used to quantitatively assess the success of an entity or activity. The KPIs an organization selects depends upon the CSF activities and how the related CGMS processes and procedures are defined and implemented. The CGMS processes and procedures tell us which items, activities, or artifacts are available to measure. The organizational-level CSFs in Table 14 should be tailored to meet the specific needs of the organization implementing the CGMS. In addition, targets and thresholds should be defined for each CSF. The targets should represent the desired value or range of values for the CSF. The thresholds should indicate the value or range of values that should trigger a change in status or the performance of a task or group of tasks.

When defining CSFs for your organization, keep in mind that CSFs are inherently hierarchical. A CSF on the executive or organization level will likely influence a very different set of CSFs on the management or division level, which will in turn drive yet another closely aligned set of CSFs for the individual.

Critical Success Factors	Descriptions	Example KPIs
Effectiveness, Composition, and Leadership of the CGMS Implementation Team	• If the implementation team is not effective, the CGMS initiative will not reach a successful conclusion. The implementation team should have a sense of urgency to keep the team focused, moving forward, and to minimize delays that can derail the initiative. • The composition of the team should consist of cross-functional stakeholder representation that includes business and IT, practitioners through executives, project/program management, and service support and delivery representation. • The team lead should have cross-functional knowledge, strong project management skills, and strong facilitator skills.	• Number of team meetings • Number of meetings within the past three months • Number of Action Items (AIs) • Average length of time AIs are open • Percentage of AIs open • Number and percentage of stakeholders represented • Percentage of IT representation by management level • Percentage of business representation by management level
Effectiveness of CGMS-Implementation Planning and Management	• The CGMS should be planned like a service that has to be continually managed and improved. Among other things, the CGMS implementation plan should define the CGMS goals and objectives, CSFs, stakeholders and stakeholder management plan, risk management plan, tasks and milestones with corresponding schedule, roles and	• Earned value • Percentage complete • Planned and actual complete dates • Planned and actual costs to date • Number of AIs • Percentage of AIs open

Critical Success Factors	Descriptions	Example KPIs
	responsibilities, and communications plan. • Project cost, schedule, scope, issues and risks, and other project parameters are defined, tracked, and managed. • Project status is routinely reported to senior and executive management.	• Milestone status
Alignment of Cloud Service Objective and Other CGMS Components	• Proper alignment of GGMS components is essential throughout the implementation of the CGMS, as well as during steady-state operations. During implementation of the CGMS, the following alignments are upheld: o Cloud service principles are aligned with requirements for effective governance and management and with the vision, mission, and values of the organization. o Cloud governance processes are aligned with principles. o As appropriate, processes align with industry standards and best practices. o Cloud service policies align with processes. o Cloud service procedures align with policies and processes. o Other process assets (e.g., checklist, templates, etc.) and tools align with processes and procedures. • Once the CGMS is implemented, it supports the continuous alignment of cloud service objectives with business and IT strategies, goals, and objectives, and with stakeholder needs. • Cloud service objectives have supporting benefits and risks that are tracked and managed	• Total number of cloud service objectives • Number and percentage of IT strategic & operational objectives mapped to cloud service objectives • Number and percentage of business strategic & operational objectives mapped to cloud service objectives • Number and percentage of stakeholder needs mapped to cloud service objectives • Process assets alignment percentage • Percentage of benefits realized • Value of benefits realized
Transparency and Stakeholder Involvement	Stakeholders are engaged in the CGMS initiative from inception through full implementation. Stakeholder buy-in is needed throughout the lifecycle of the CGMS, from the establishment of the charter, to approval of new or revised processes and procedures, to routine performance reporting. Stakeholder engagement is planned and managed.	• Number of stakeholder requirements by stakeholder type (e.g., key, primary, etc.) • Percentage of stakeholder requirements met

Critical Success Factors	Descriptions	Example KPIs
Risk Management	Risks to a successful CGMS implementation are defined tracked, and managed to closure. Serious and threatening risks are communicated to the executive management team.	• Number of serious risks opened and closed • Number of threating risks opened and closed by type (e.g., security, compliance, etc.) • Average risk rating by type
Appropriateness of Process Infrastructure	The process infrastructure consists of documented policies, processes, procedures, templates, checklist and other such items. The process infrastructure established to support the CGMS is agile, doable, and sustainable for the organization.	• Number of processes within CGMS • Number of full process assessments within the past 30 days and within the past 90 days • Average procedure execution time • Longest procedure
Organizational Awareness and Preparation	Stakeholders are appropriately trained on the CGMS and how to perform assigned tasks.	• Average training evaluation rating overall and by process • Total number of training requirements • Percentage of open training requirements

Table 14: Example of CGMS Implementation Critical Success Factors and Key Performance Indicators

Institutionalize

Once the CSMS is implemented it has to be institutionalized and continually improved. Institutionalization implies that a process is ingrained in the way that work is performed and there is commitment and consistency in performing (i.e., executing) the process (CMU, 2010, p. 57). Essentially, institutionalized processes have become a routine way of doing business.

A stable and effective assessment process is necessary to obtain and sustain institutionalization. If CGMS process-and-procedure compliance is not routinely assessed, it is unlikely an organization will consistently use new or revised processes and procedures, particularly if they represent a departure from organizational norms. Once processes and procedures have been developed or revised, approved, and properly released for use, stakeholders have to be informed and appropriately trained. Process compliance assessments are then needed to ensure the processes are being used consistently and correctly. The results of assessments should yield corrective and/or preventative actions, process improvement recommendations, and process performance data. Assessment outputs/results must be tracked to closure, resulting in a CGMS that will continually increase its level of institutionalization and capability.

For processes and procedures to remain institutionalized, as requirements and objectives for the CGMS change and improvements are introduced; policies, processes, and procedures must be reviewed for impacts resulting from proposed changes and revised as appropriate.

A PI team is necessary to manage changes to all process assets and ensure the CGMS remains aligned to the needs and objectives of the organization. As appropriate, changes to CGMS process assets should be reviewed and approved by affected stakeholders. The use of revised processes and procedures must then be introduced and communicated throughout the organization in a structured manner.

Another characteristic of an organization with institutionalized, sustainable processes is an organizational training and awareness program that is planned and managed. The training plan should address training needs and how they are defined, tracked, and managed. There should also be a designated training manager or coordinator to manage the training and awareness program. The training coordinator should be a member of the CPIT or work closely with the team to identify, coordinate, and address training needs. As the CGMS changes, the training and awareness coordinator must make sure that changes are absorbed into the training requirements, and affected stakeholders are appropriately informed or trained on the updates. Figure 18 is an actual training dashboard from a previous client. The dashboard shows training requirements that are a roll-up of individual requirements defined on a worksheet within an excel workbook. The dashboard illustrates a summary of organizational training requirements that are tracked by the role an individual holds within the organization. A similar tracking tool is needed to ensure everyone that has a role within the CGMS receives the appropriate training and training status is reported to senior management.

Figure 18: Example of Tracking Training Requirements

Final Thoughts

In a 2012 early adopter, lessons-learned study conducted by Forrester Consulting and commissioned by Oracle, 156 senior IT decision-makers with cloud responsibilities were surveyed. Of the respondents, 98% had major cloud application management issues, and 90% believe that managing the transition of critical business applications to the cloud was a major challenge (Forrester, 2012). These results strongly imply that organizations are implementing cloud services without the appropriate due diligence to adapt their existing governance and management capabilities to support cloud services.

One of the biggest consequences of not having the appropriate governance and ITSM capabilities for new technology adoptions, is that the condition creates serial issues. And if not addressed, at best the issues become a normal, more costly, less effective way of doing business.

Designing, establishing, and/or evolving IT governance and management process architectures to support cloud services should be a part of the cloud-adoption-planning process. Allowing technology adoption to outpace process adaption significantly increases the risk of your cloud services' initiative failing.

References

[1] Software Engineering Institute (SEI). (2010). CMMI® for Services, Version 1.3. MA: Carnegie Mellon University (CMU).

[2] Cloud Security Alliance. (2010). Domain 12: Guidance for Identity & Access Management V2.1. Author.

[3] Richard A. Caralli. (2004). The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management. Cambridge, MA: CMU.

[4] Forrester Consulting. (2012). Enterprise Cloud: Lessons Learned From Early Adopters. Cambridge, MA: Forrester Consulting.

[5] Roger Grimes. Staying Secure in the Cloud. InfoWorld Deep, Cloud Security: A New Security Model for the Cloud ERA

[6] J.C. Henderson, N. Venkatraman. (1993). Strategic Alignment: Leveraging Information Technology for Transforming Organizations. IBM Systems Journal, vol. 32, no. 1.

[7] Michael Hogan, Fang Liu, Annie Sokol, Jin Tong. (2011). NIST Cloud Computing Standards Roadmap. Gaithersburg, MD: National Institute of Standards and Technology.

[8] Information Systems Audit and Control Association (ISACA). (2012). COBIT 5 Implementation. IL.: Author.

[9] International Organization of Standardization (ISO). (2008). ISO/IEC 38500: Corporate Governance of Information Technology. Geneva: Author.

[10] ISACA. (2014). CGIT Review Manual 2014: Certified in the Governance of Enterprise IT. Rolling Meadows, IL.: Author

[11] ISACA. (2012). COBIT 5 A Business Framework for the Governance and Management of Enterprise IT. Rolling Meadows, IL.: Author

[12] John P. Kotter. (1996). Leading Change. Boston, MA: Harvard Business School Press.

[13] Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger and Dawn Leaf. (2011). NIST Cloud Computing Reference Architecture. Gaithersburg, MD: National Institute of Standards and Technology.

[14] Price Waterhouse Cooper. (2014). Managing the Shadow Cloud: Integrating Cloud Governance into Your Existing Compliance Program. Author.

[15] Peter Weill, Jeanne W. Ross. (2004). IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. [Kindle DX version]. Retrieved from http://www.amazon.com.

ABOUT VIDERITY

Viderity provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build, and run those solutions in a way that delivers bottom-line value.

To learn more visit: Viderity.com

ABOUT THE AUTHOR:

Rachel Everett is a results-driven technology services company founder, thought leader, and digital executive with nearly 20 years of experience leading flagship digital transformation programs. She is passionate about helping organizations grow their audience and gain technological and organizational efficiencies through digital transformation. Research and editing of this report was supported by Rachel's teams at Viderity that specialize in information technology related strategy and governance.

To connect with Rachel Everett: https://www.linkedin.com/in/racheleverett/

VIDERITY

STRATEGIC, CREATIVE, TECHNICAL

www.viderity.com