An Overview of Enterprise Cloud Strategy Approaches and a Pragmatic Template for Setting Your Cloud Use Policy

Published: 25 January 2017 **ID:** G00317697

Analyst(s): *Gregor Petri | Neville Cannon*

Summary

With the increasing popularity of external cloud services, enterprises struggle to maintain comprehensive cloud use policies, limiting strategic adoption. IT Infrastructure & Operations leaders can use this template to bridge and unify cloud strategy and cloud policy.

More on This Topic

This is part of an in-depth collection of research. See the collection:

SERIES OVERVIEW

Guide to Gartner's Research on CSP Security (https://www.gartner.com/document/code/340465?ref=grbody&refval=3582218)

Overview

Key Challenges

Enterprise IT departments often develop a cloud strategy to guide their plans regarding adoption of infrastructure as a service (IaaS) and platform as a service (PaaS), while they issue cloud policies to control (and often limit) the use of SaaS by line-of-business departments.

The advent of SaaS has made it easy for departments to act independently, increasing organizational risk through the circumvention of IT review, data management and approval processes.

IT departments tend to overregulate cloud adoption by line-of-business departments by overstating the risks while demanding too much control. Such poorly drafted cloud use policies can give a false sense of security to CIOs and senior managers.

Recommendations

IT Infrastructure & Operations leaders responsible for governing cloud market opportunities and adoption should:

Ensure strategy and policy logically fit together and drive correct behavior, preferably through facilitation rather than regulation. To achieve this, use constructive, clear and direct language.

Review existing or proposed cloud strategies and usage policies against this research to identify relevant gaps; validate your approach and deliver pragmatic guidance.

Take a differentiated — in many cases, bimodal — approach toward cloud adoption, by balancing risk and due diligence with rapid acquisition and deployment of cloud services.

Strategic Planning Assumptions

Through 2018, the biggest inhibitor to internal cloud service brokerage (CSB) success will be organizational and business process challenges — not technology. [1] (#dv_1_predicts_2014)

By 2020, anything other than a cloud-only strategy for new IT initiatives will require justification at more than 30% of large enterprise organizations. [2] (#dv_2_predicts_2017)

By 2018, 50% of the applications hosted in the public cloud will be considered mission-critical by the organizations that use them. [3] (#dv_3_2017_planning)

Introduction

As enterprises try to further raise their innovation capabilities and their general level of agility, adoption of cloud services is accelerating rapidly (see "Predicts 2017: Cloud Computing Enters Its Second Decade" (https://www.gartner.com/document/code/311365?ref=grbody&refval=3582218)) Its appeal as a source of elastic services or computing power means that many business units bypass traditional IT procedures. This may create a "shadow" IT environment that lacks the oversight necessary for critical data and services.

Attempts to develop cloud usage policies in isolation of cloud strategy can become confused and obstructive. The IT department can be viewed as draconian or restrictive in limiting a business department's freedom to operate or innovate. Craft policies to highlight the positive uses of cloud and to encourage adoption; place these within a firm but fair set of guidelines that leverage a set of agreed simple principles (see Note 1).

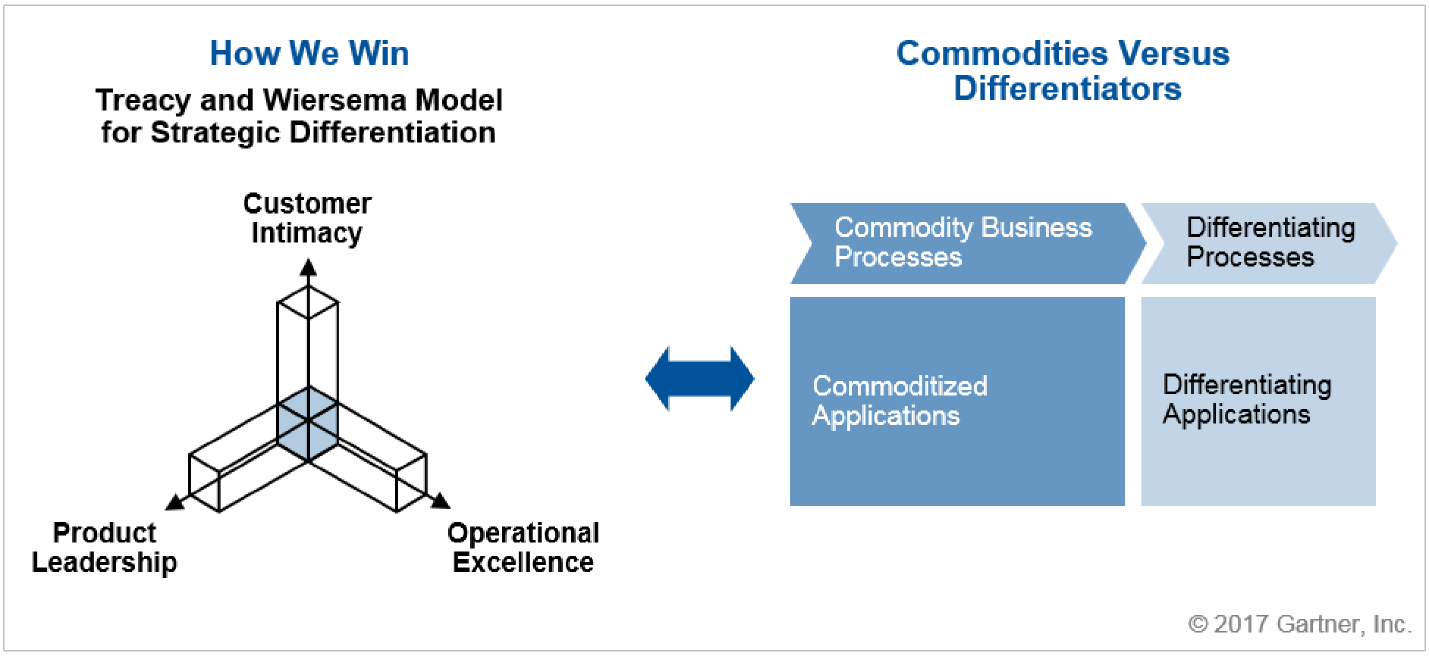
A cloud usage policy should be complementary to cloud strategy. It should help the business decide what to do and why. The policy must help explain to workers across the organization how to act — within and according to the strategy — while allowing for a differentiated approach based on the specifics of the use case. For a sample policy template, see Note 2 for a template derived from Gartner, previously published in "Government Cloud Use Policy Template." (https://www.gartner.com/document/code/302208?ref=grbody&refval=3582218) For a strategy template, see Gartner's Research for Technology Professionals "Designing a Cloud Strategy Document." (https://www.gartner.com/document/code/311458?ref=grbody&refval=3582218&latest=true)

Analysis

Corporate Strategy Trumps Cloud Strategy

As highlighted in the diagram in Figure 1 (from "The Art of the One-Page Strategy," (https://www.gartner.com/document/code/281842?ref=grbody&refval=3582218)) any IT strategy has to align with corporate strategy. This is especially true for cloud strategies. If the corporate goal, for example, is to become a recognized leader in customer intimacy and customer experience, then a lift-and-shift-oriented cloud strategy that mainly pursues potential cost savings around established internally focused functionality can at best be complementary, but is very unlikely to be supportive — or even strategic — in context of the enterprise strategy.

Figure 1. Use Corporate Strategy as a Lens for Cloud Strategy


How We Win
Treacy and Wiersema Model for Strategic Differentiation
Customer Intimacy
Product Leadership
Operational Excellence
Commodities Versus Differentiators
Commodity Business Processes
Differentiating Processes
Commoditized Applications
Differentiating Applications
© 2017 Gartner, Inc.

Source: Gartner (January 2017)

It is also important to note that cloud adoption, as such, is not a goal, and thus any cloud strategy should support higher business level objectives and strategies. This means that most organizations will not be able to define a single "one size fits all" cloud strategy. Therefore, it is important — as the right of the diagram in Figure 1 indicates — to distinguish between differentiating and commodity processes and to align your strategies for cloud adoption with these different types of processes. This can result in a bimodal approach to adopting cloud or — an even more pragmatic, common practice among early cloud adopters — aligning the types of cloud services being considered with Gartner's pace-layering classification of:

Systems of record (offering standard commodity functions that many companies use).

Systems of differentiation (offering value unique to the company).

Systems of innovation (new functions to experiment with).

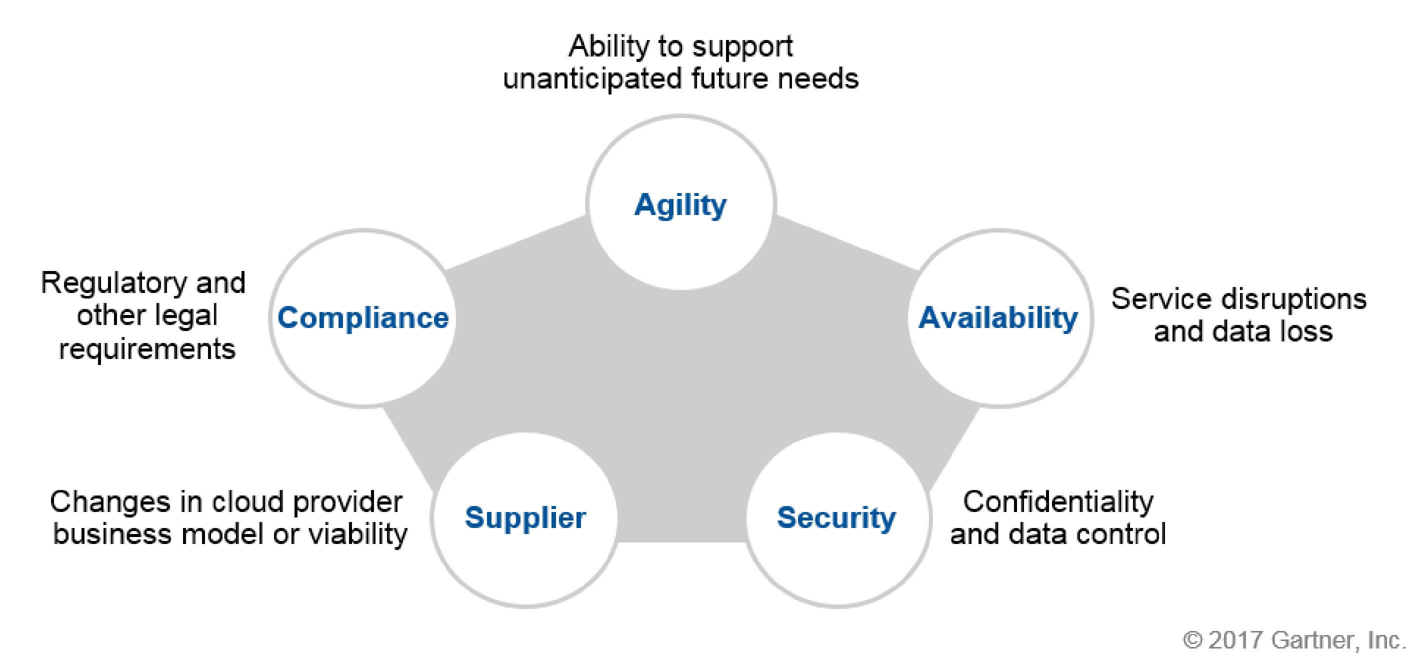
Here the type of cloud service has to match the characteristics of the business process. For example, for systems of record, a standard off-the-shelf SaaS service can offer the required functionality while requiring very limited effort of the organization. For systems of differentiation, the flexibility that platform-as-a-service (PaaS) offers can be ideal. This is not to suggest that one type of cloud is only suitable for one type of process and not any other. For systems of innovation, for example, SaaS can be a fast way to enable an end-user pilot without the need to install or master any technology upfront, while at the same time IaaS can enable fast IT experimentation with the technology. (For more background on pace layering, see "How to Develop a Pace-Layered Application Strategy." (https://www.gartner.com/document/code/276478?ref=grbody&refval=3582218))

Balanced Risk Management

Any process for setting cloud strategy must assess the possible risks regarding aspects such as security, agility, supplier, availability and compliance, then weigh these against the potential benefits for the business in a balanced and compliant manner. Risk management is still mentioned by many Gartner clients as one of the aspects of cloud computing that remains the hardest to build consensus and a common approach around.

Gartner's recommended approach for cloud risk management is discussed in "A Public Cloud Risk Model: Accepting Cloud Risk Is OK, Ignoring Cloud Risk Is Tragic." (https://www.gartner.com/document/code/315668?ref=grbody&refval=3582218)

Figure 2. Base Your Cloud Usage Decisions Around These Public Cloud Risk Domains


Ability to support unanticipated future needs
Agility
Regulatory and other legal requirements
Compliance
Availability
Service disruptions and data loss
Changes in cloud provider business model or viability
Supplier
Security
Confidentiality and data control
© 2017 Gartner, Inc.

Source: Gartner (January 2017)

Risk management has to be an integral part of any cloud strategy process and the long-promoted best practice of formulating specific cloud exit strategies (and the associated risks of such an exit) before committing to any cloud project or vendor risk management continues to be an essential step in reaching balanced cloud deployment decisions.

Within cloud risk management, overall the area that Gartner receives most questions about is how to approach the assessment of the security measures of individual cloud providers. In "How to Evaluate Cloud Service Provider Security," (https://www.gartner.com/document/code/295291?ref=grbody&refval=3582218) we provide guidance, highlighting also how "one size fits all" approaches are inefficient and ineffective, and are likely to result in bad choices for public cloud use.

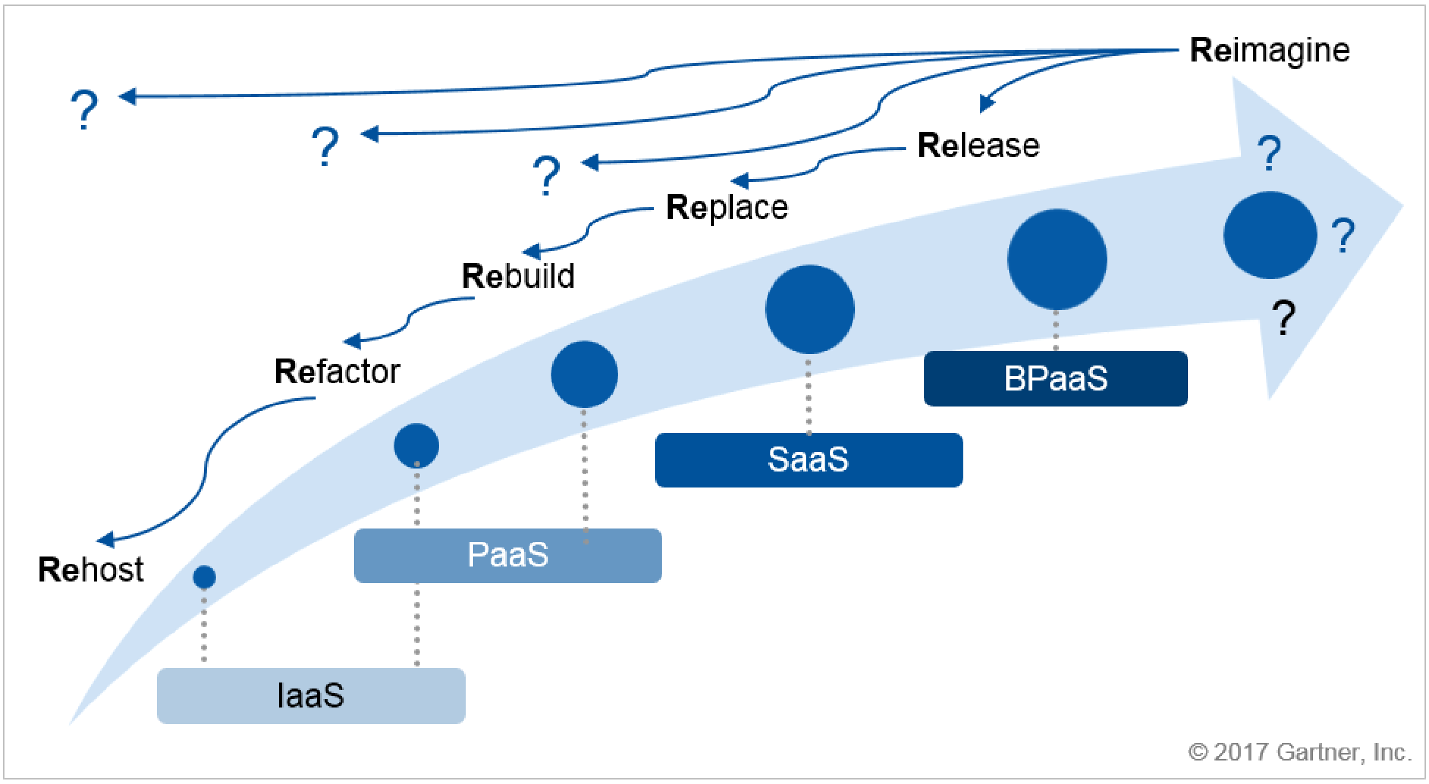
Specify Your Potential Routes to the Cloud in Cloud Playbooks

When discussing cloud strategy and establishing subsequent policies for cloud computing, it is important to differentiate guidance by the various possible routes to the cloud, such as:

- Are you rehosting an application "as-is" (lift-and-shift) on cloud infrastructure as a service?
- Are you refactoring (or even rebuilding/recoding) an application to fully take advantage of the new environment and platform to — as a result — become more agile or less costly?
- Are you replacing an existing system with a ready-made SaaS application (and abandoning the current system)?
- Are you releasing (or relinquishing) a formerly internal business process (such as invoicing, payment collection or salary administration) to an external business process-as-a-service (BPaaS) provider?

Alternatively, are we reimagining the way the enterprise operates with new capabilities? For example, by moving the organization from a linear supply chain transformation process to a multienterprise platform, as described in "Building a Digital Business Technology Platform." (https://www.gartner.com/document/code/297286?ref=grbody&refval=3582218)

Figure 3. Different Routes to the Cloud and the Top-Down Decision Tree



BPaaS = business process as a service; IaaS = infrastructure as a service; PaaS = platform as a service; SaaS = software as a service

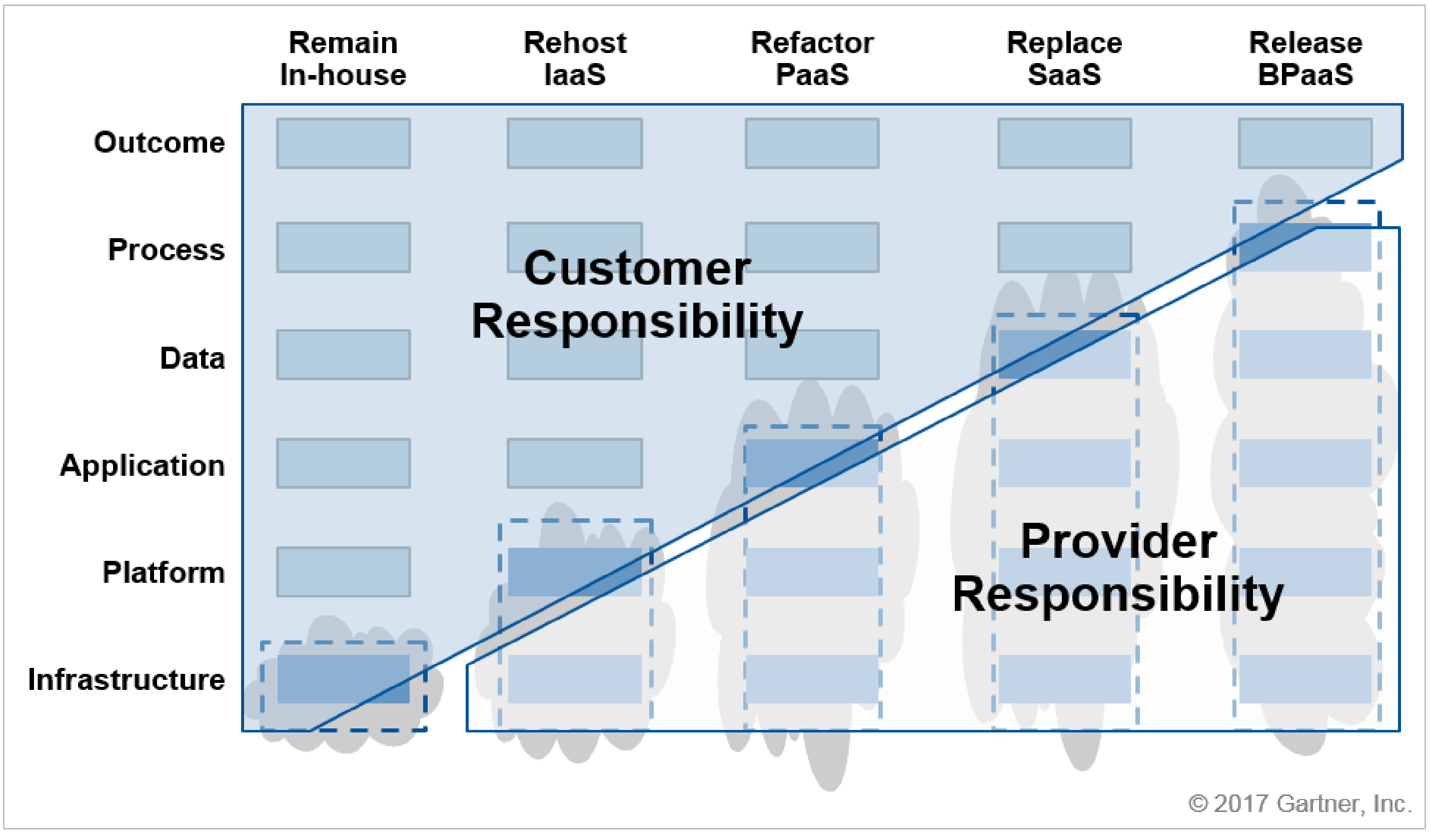
Source: Gartner (January 2017)

For each of the different scenarios, it makes sense to have thought about the way the company wants to approach these and to document the common or preferred approach for each scenario in a type of playbook. A playbook does not equate one-to-one to a cloud service model (IaaS, PaaS, SaaS) as the approach for building a new application on top of IaaS using a DevOps approach can be very different from the preferred approach for lifting and shifting a legacy application with as little effort as possible. For example, in the former, the DevOps team may want to optimally use all the native capabilities that their IaaS provider of choice offers (as time to market may be critical). While for lift-and-shift of legacy workloads, they may want to limit cloud feature dependency by mandating the use of a third-party cloud management platform that enables portability (as applications migrated with minimal refactoring or re-engineering are unlikely to reap any benefits of proprietary cloud capabilities anyhow).

Use a Simple Decision Tree

The main arrow in the diagram in Figure 3 illustrates how — from a technical hierarchy perspective — higher-level services (such as SaaS and BPaaS) are often built on top of lower-level cloud services (such as IaaS and PaaS) or even still on precloud infrastructures. This, however, does not imply that enterprises start at the bottom and move up from there; the recommended decision path in most cases should be the reverse — namely top-down.

Figure 4. Understanding Customer Versus Provider Responsibilities



BPaaS = business process as a service; IaaS = infrastructure as a service; PaaS = platform as a service; SaaS = software as a service

Source: Gartner (January 2017)

Before even contemplating rehosting or refactoring an application, start by asking what the organization may look like in the future (for example, as a digital business) and whether the supported business process is still required (or still performed internally) by then. For a given process, the decision tree could look like this:

Do you need this process long term? (If not, how to gracefully fade it out and, more importantly, what new processes do you need to prepare for?)

Do you need/want to perform the process in-house? (If not, consider BPaaS.)

Can you simply consume the required functionality for this process as SaaS?

If you need more flexibility, can you customize (using PaaS) or run it yourself, but avoid having to manage a full middleware stack (again PaaS)?

If you need to run it yourself on bare infrastructure, can you use a shared (public or hosted private) infrastructure service (IaaS)?

Additionally, in increasingly rare cases:

If no such service is available (or allowed by your regulator), can you run one internally using (open) standard hardware and software?

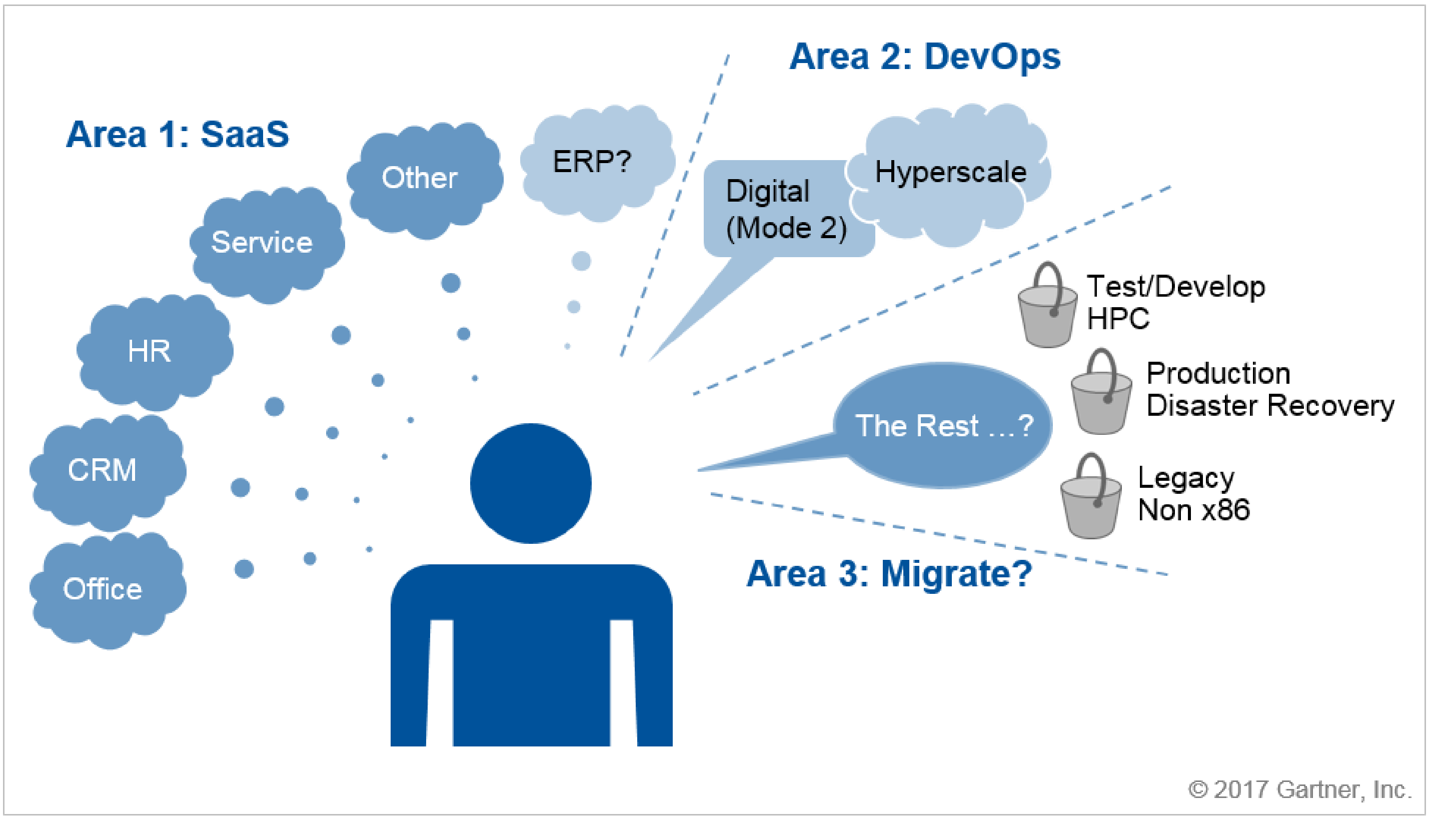
If you need software or hardware capabilities that are now available, can you create (or contract) these, based on your own specifications?

The last option will become increasingly rare, similar to how we saw companies needing to build their own compilers or database management systems that become more an exception than the rule. Again, this will not be a companywide decision across all cloud deployments. The decision tree has to be traversed for each (type of) use case. For a large and increasing number it will lead to SaaS, for some (typically the more unique/differentiating ones) it may lead to IaaS or PaaS (or the combination of IaaS+PaaS).

Cloud Strategies and Policies Must Address All Cloud Models

Gartner has observed in many enterprises, that the organization concentrates on the use of IaaS and PaaS (by the IT organization) when it comes to cloud strategy. In contrast, cloud policy tends to cover the adoption of SaaS (by end-user departments). In many cases, it is better if both strategy and policy cover the wider cloud portfolio in order to offer guidance that is more comprehensive.

Figure 5. Typical Enterprise Cloud Adoption Areas



CRM = customer relationship management; ERP = enterprise resource planning; HPC = high-performance computing; HR = human resources; SaaS = software as a service

Source: Gartner (January 2017)

We described the leading role that SaaS plays in cloud adoption in "Three Factors Will Continue to Impact Enterprise Cloud Playbooks" (https://www.gartner.com/document/code/271075?ref=grbody&refval=3582218) and more recently in "The CIO's Journey to Cloud SaaS: An 'All in, Flip' Strategy." (https://www.gartner.com/document/code/313263?ref=grbody&refval=3582218) The cloud adoption of most organizations has so far developed around three major areas (also see Figure 2):

1. The first pertains to the accelerating adoption of SaaS solutions in common areas such as CRM, HR, cloud-based office solutions, service desk, or travel and expense management.

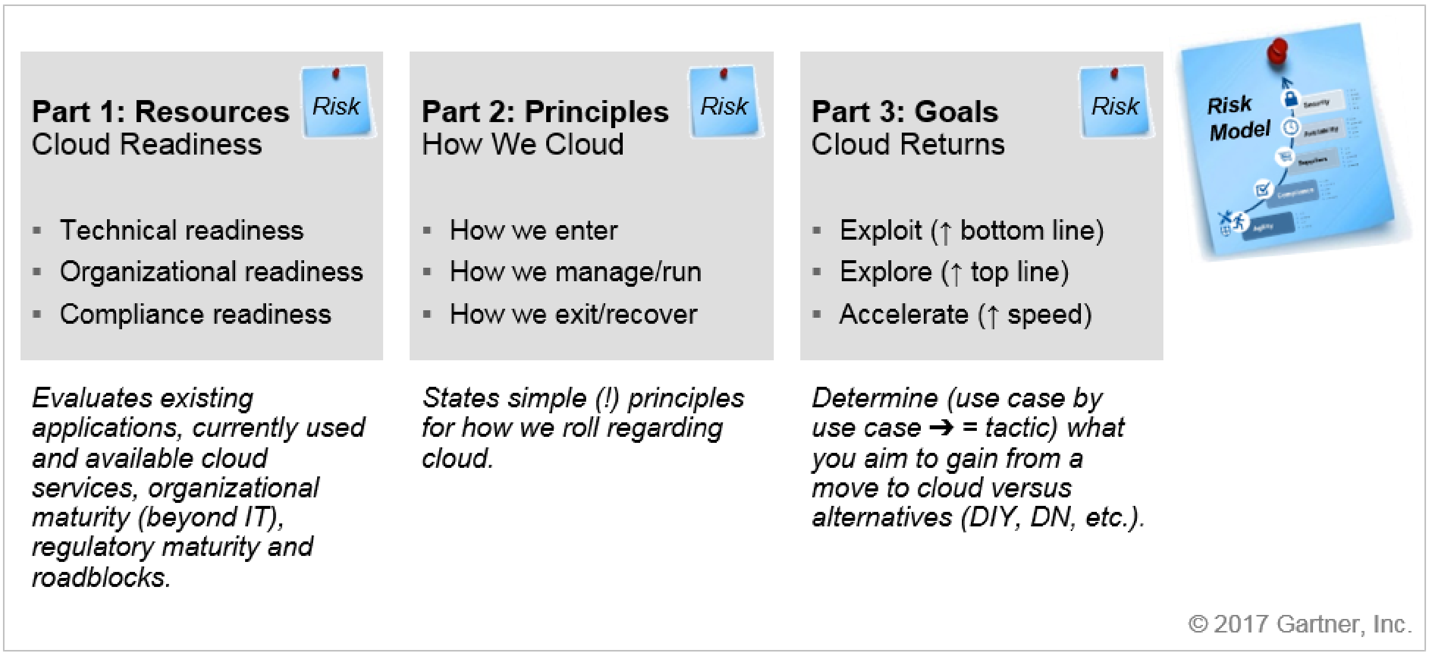
2. The second area is the development of new differentiating — in most cases, end consumer-facing — applications that must scale and transform in a similar agile and dynamic fashion, as consumer-oriented social media applications. (See "Use Web-Scale IT to Make Enterprise IT Competitive With the Cloud" (https://www.gartner.com/document/code/271925?ref=grbody&refval=3582218) and "Web-Scale IT Empowers Teams to Create a Culture of Innovation." (https://www.gartner.com/document/code/251066?ref=grbody&refval=3582218)) These new web-scale applications are increasingly deployed on top of public cloud offerings of hyperscale IaaS and IaaS+PaaS providers.

3. The third area is often the primary area of attention for enterprise IT infrastructure teams, it involves the migration of existing on-premises workloads to the cloud. Initial workloads and processes to migrate are typically test and development, high-performance batch and simulation workloads, as well as disaster recovery and backup. However, with an increasing number of internal applications being replaced by SaaS and new applications deployed predominantly being deployed on public hyperscale platforms, enterprises have started to evaluate what to do with the production workloads now remaining in their traditional data centers.

Setting Some Cloud Principles

Given the wide variety of deployments, use cases and pace layer types, it is natural that one cannot address all these with one simple generic cloud strategy. A pragmatic way to address this is described in "A Three-Part Approach to Jump-Start Your Cloud Strategy." (https://www.gartner.com/document/code/292590?ref=grbody&refval=3582218)

Figure 6. A Three-Part Approach to Cloud Strategy



Part 1: Resources
Cloud Readiness

- Technical readiness
- Organizational readiness
- Compliance readiness

Evaluates existing applications, currently used and available cloud services, organizational maturity (beyond IT), regulatory maturity and roadblocks.

Part 2: Principles
How We Cloud

- How we enter
- How we manage/run
- How we exit/recover

States simple (!) principles for how we roll regarding cloud.

Part 3: Goals
Cloud Returns

- Exploit (↑ bottom line)
- Explore (↑ top line)
- Accelerate (↑ speed)

Determine (use case by use case ➔ = tactic) what you aim to gain from a move to cloud versus alternatives (DIY, DN, etc.).

© 2017 Gartner, Inc.

DIY = do-it-yourself; DN = do nothing

Source: Gartner (January 2017)

In this quick three-step approach, the process begins with:

1. Taking inventory of cloud readiness. (How ready are your people, your applications and your regulators?)

2. Agreeing some simple principles (such as "all customer data must always be encrypted" or "all data must be stored within the European Union"). Gartner has observed that companies that started with some simple principles around cloud, found it much easier to subsequently develop a comprehensive strategy with accompanying policies.

3. Formulating the goals or returns (since cloud is not the aspiration but a means to achieve higher goals such as increasing speed, or improving bottom-line [reduce cost] or top-line [increase revenue]).

In addition to the simple decision model for adopting external cloud services, Gartner provides a more in-depth approach to formulating a cloud strategy (including the option for private cloud) in "Devise an Effective Cloud Computing Strategy by Answering Five Key Questions." (https://www.gartner.com/document/code/270415?ref=grbody&refval=3582218) (See Note 3 for our questions and recommendations.) In addition, Gartner for Technology Professionals service offer a body of cloud-planning research, supporting technology professionals (such as cloud architects), a rapidly emerging role in Gartner customer organizations (see Note 4).

The Changing Role of the IT Department

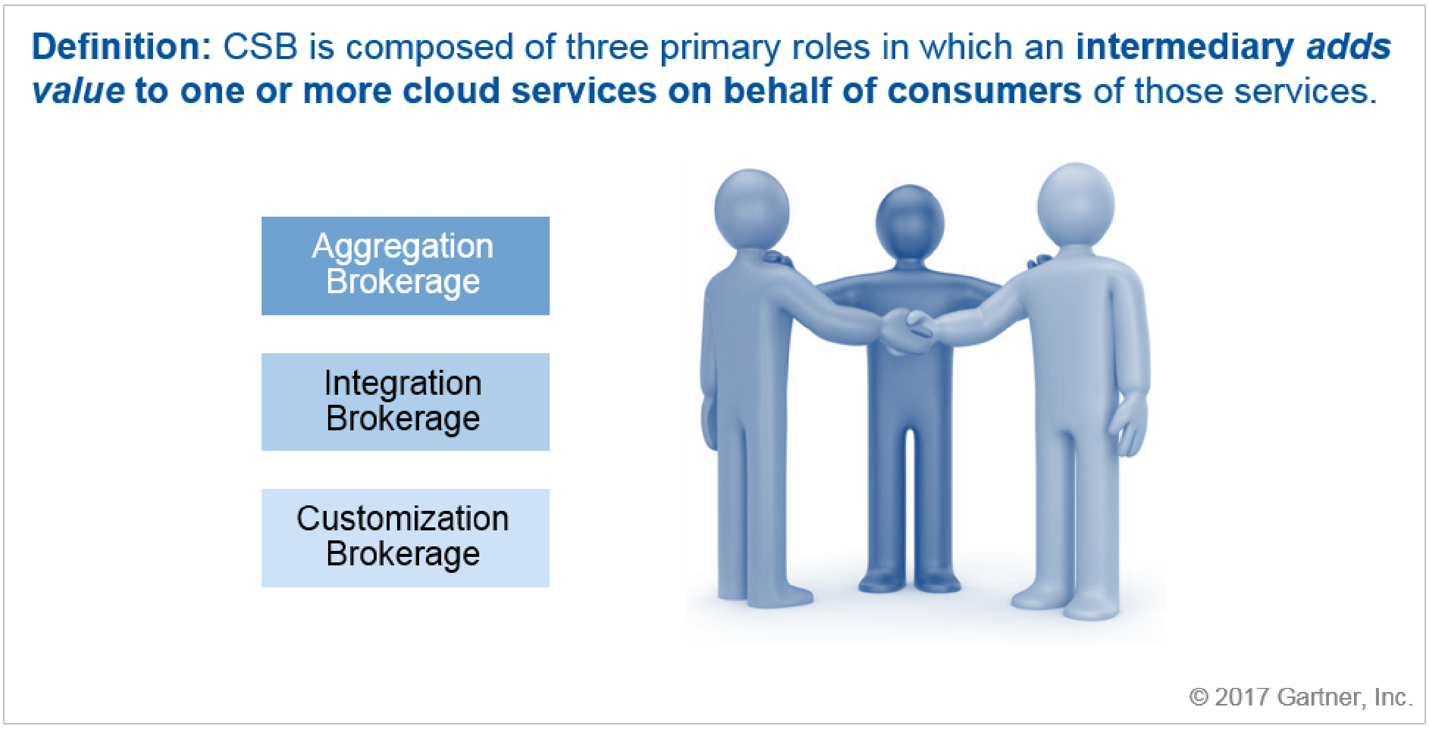
The impact of any cloud adoption or migration will be a changing role for the internal IT organization, and also here, we will see that this role will need to be differentiated for different types of services. Typically, this involves the addition of an IT services broker group that liaises between business stakeholders and internal specialized IT groups. Stakeholders include business leaders, end users and application owners (including DevOps teams) that — especially for Mode 2 type of applications — prefer a self-service-oriented relationship. Internal specialized IT groups focus on:

1. Management of the traditional IT environment and associated applications

2. Management of critical workloads on private — and increasingly on public — cloud infrastructure and platform services

3. Management of the (many relationships with) public cloud service providers

Figure 7. Three Primary Roles of CSB



Definition: CSB is composed of three primary roles in which an **intermediary *adds value*** **to one or more cloud services on behalf of consumers** of those services.

Aggregation Brokerage

Integration Brokerage

Customization Brokerage

© 2017 Gartner, Inc.

CSB = cloud service brokerage

Source: Gartner (January 2017)

However, as we described in "Predicts 2014: Cloud Services Brokerage," (https://www.gartner.com/document/code/258083?ref=grbody&refval=3582218) we still feel that through to 2018 the biggest inhibitor to internal CSB success will be organizational and business process challenges — not technology — with the new role of IT being quite comparable to the role of HR. This means less direct involvement in day-to-day operations, as digital line of business departments and their DevOps teams will deploy and manage their cloud services (increasingly through self-service). They will, however, retain direct involvement in (vendor) selection, background checks, contracting, on- and subsequent off-boarding, recovery planning, as well as in management and monitoring of overall performance, costs and budgets. In addition, IT departments will remain responsible for relevant training, awareness and education, including a number of companywide foundational services.

From Strategy to Policy

Ensure your policy drives behavior consistent with your strategy by using constructive, direct language. Unintended consequences following the introduction of any new policy or update can occur. However, the likelihood of an adverse impact can be minimized by making transparent how the policy is expected to support the underlying cloud strategy. Considering what people may do or how they may react as a result of the new policy will help ensure that obvious drafting issues are avoided (see "Culture Change Is Easier Than You Think" (https://www.gartner.com/document/code/276736?ref=grbody&refval=3582218)).

The following highlights areas that IT leaders who draft policies may wish to consider.

Become a Facilitator Not a Regulator.

Heavily regulated industries have a higher necessity to demonstrate control and compliance than some other sectors. Many IT and security executives think that retaining the IT role as "policeman" is important in reducing risks to the organization. However, this perception can be a fallacy when witnessing the extraordinary growth of shadow IT. We advise a balanced approach (the carrot-and-stick), for example, by offering a portal with freely accessible approved cloud services, supporting convenient single sign-on (the carrot) but also mandating that end-user departments register all services they adopt in a central register and checking for compliance by using a cloud access security broker (CASB) to identify rogue services (the stick).

Desist From Overly Promoting Risk Avoidance.

Enterprises increasingly desire to become more agile, better able to flex and adapt to a changing market. Processes that are overly bureaucratic and cumbersome will be difficult and slow to amend. This can be exacerbated if the organization is risk-averse. For an organization to be able to behave in an agile manner, its processes must be lean, also its policies and procedures must follow suit.

If the organization is risk-averse or the IT department is lacking vision, then any cloud policy will likely be drafted from a defensive posture. This increases the likelihood of a policy full of jargon and bureaucratic processes, with tough controls that severely limit migration to the cloud. The resulting tough authorization process is often not scalable to the task in hand, and the antithesis of how Gartner suggests you should empower business users to manage shadow IT (see "Embracing and Creating Value From Shadow IT" (https://www.gartner.com/document/code/264121?ref=grbody&refval=3582218)). The corollary of this is that business departments continue to circumvent the process and policy, thereby undermining the reason for policies to exist, which is to encourage a consistent, compliant approach across the organization.

Address the Fears Within IT and Fight the Desire to Exert Control at Every Level.

Accept that shadow IT is here and, while exploring the risk profile with senior leadership, provide business users with the guidelines and support necessary for them to make informed decisions. Having different approaches for different situations will be a vital component in the move toward becoming a bimodal organization. Harnessing innovation, while providing necessary guidelines to ensure integration with existing architecture and applications, remains practical.

CIOs must question the procedures suggested or those already in place to determine if they are fit for purpose. Are they diligent from the IT department's point of view, and will they scale to take account of the latent demand within the organization? If the honest answer is no, then the process is not fit for purpose. Do not believe otherwise. Revisit the process and amend as necessary, until it can scale.

Enlist Procurement Staff Support.

By involving procurement staff from the beginning of this process, it will become easier to understand and implement necessary changes in existing procurement policies and practices. Moving to the cloud should not be seen solely as a technical decision for the IT department; nor should the procurement of a SaaS application be solely for the line-of-business department. All departments must be engaged with the implementation of the cloud strategy if benefits are to be realized.

Be Direct and Constructive.

Policies and the prevailing culture must reflect a positive approach and attitude. Avoid a stance and language style that appear negative and controlling. A disapproving tone is easy to inject into policy documents without, perhaps, meaning to.

Gain Support Early.

Socializing draft policies among business users can help guide the authors to the correct tone of language and style to make the policies more acceptable. Listen to the feedback you receive at this stage. Ensure that you have an ongoing mechanism to capture feedback once the policy has been published.

Review.

Any policy must address relevant issues within the business, such as organizational compliance requirements and data protection, including data ownership and integration. It must also reflect the risk appetite of the business toward authorization for the adoption of cloud services.

The policy should be clear, simple and specific, providing comprehensive guidance to those making decisions. It must answer three basic questions:

"What do I have to do?"

"What must I comply with?"

"Where can I get help?"

A fourth may be relevant for managers and other IT leaders — "Who do I have to tell?"

Acronym Key and Glossary Terms

BPaaS	business process as a service
CIO	chief information officer
CRM	customer relationship management
CSB	cloud service brokerage
DIY	do-it-yourself

DN	do nothing
ERP	enterprise resource planning
FISMA	Federal Information Security Management Act (U.S.)
HIPAA	Health Insurance Portability and Accountability Act (U.S.)
HPC	high-performance computing
HR	human resources
IaaS	infrastructure as a service
ICT	information and communication technology
IEC	International Electrotechnical Commission
IG	information governance
ISO	International Organization for Standardization
PaaS	platform as a service
SaaS	software as a service
TCO	total cost of ownership

Gartner Recommended Reading

"Government Cloud Use Policy Template" (https://www.gartner.com/document/code/302208?ref=ggrec&refval=3582218)

Additional Gartner Recommended Reading Outside Your Current Subscriptions

"Toolkit: How to Create a One-Page Midmarket Cloud Strategy" (https://www.gartner.com/document/code/259533?ref=ggrec&refval=3582218)

Evidence

[1] "Predicts 2014: Cloud Services Brokerage." (https://www.gartner.com/document/code/258083?ref=grbody&refval=3582218)

[2] "Predicts 2017: Cloud Computing Enters Its Second Decade." (https://www.gartner.com/document/code/311365?ref=grbody&refval=3582218)

[3] "2017 Planning Guide for Cloud Computing" (https://www.gartner.com/document/code/311457?ref=grbody&refval=3582218&latest=true)

Note 1

Policy Guidelines

There are some basic guidelines for writing policy documents that will help make them more readable — thereby increasing compliance:

Follow your organization's template (if you have one).

Keep your policy as short as practical.

Use language that is simple, clear and concise.

Avoid the use of technical jargon; write for the audience you want to read it — not the IT staff.

Avoid too much description in the body text; if necessary, include definitions in an appendix.

Be clear about what is obligated and what is discretionary, that is must/must not or may/should.

Develop a consistent method for naming policies to make them easy to find. Names should be relatively short and specific.

Utilize any organization coding standard to assist with filing.

Identify the policy owner — name, job title and contact details.

Note 2
Cloud Policy Sample Template

Policies are important to the success of any organization. They create a consistent level of IT delivery. Adopt a method that fits within your culture to achieve this goal. In organizations with well-defined roles and responsibilities and a consistent culture, often fewer policies are required to achieve the desired levels of performance, because processes are clear and well defined. Adapt your approach and rigor to your culture and level of process maturity.

Please Note: Gartner does not provide legal advice, so the wording below should not be relied upon to be binding in contractual terms. Where this is required, consult your legal team or lawyers. Seek specific legal advice for your particular jurisdiction.

Table 1. Cloud Policy Sample Template

Section	Guide and Suggested Wording
Introduction	To inform the reader of why this policy was issued. A brief summary of its objectives and information it contains. **Example:** Since [*Date*], [*Organization Name*] has pursued the aim of making its departments more agile and flexible through the adoption of cloud-based technology. It seeks to minimize its ownership of technical infrastructure and move toward a consumption-based model, giving it the ability to more rapidly adapt to changing circumstances, user needs and budgetary pressures when they arise. [*Organization Name*] is implementing the policy, skills and tools necessary to accelerate the adoption to cloud and to become less technology-centric and more outcome-focused.
Purpose	One or two sentences that clearly state what the policy is seeking to achieve. **Example:** This policy is to stimulate the widespread adoption of cloud-based services across [*Organization Name*]. The intention is to move away from ownership of ICT infrastructure and toward the adoption of a consumption-based model for IT software and infrastructure.
Authority	If appropriate, identify under what authority this policy operates. **Example:** Corporate data policy [*ABC 123456 XYZ*] states that policies impacting the electronic transmission of data must be risk assessed and that interoperability must be maintained across all relevant systems.
Policy	Set out the intended direction and the actions necessary for the organization, following adoption of this policy. **Example:** **Procurement and Sourcing** This policy requires that an adoption of cloud-based services is initially and routinely explored whenever a system is being considered for replacement. Application end-of-life planning must plan for the adoption, wherever practicable, of cloud-based replacements. Where possible, enterprise purchasing policies should be used. These can be found at [*Insert location and details of appropriate framework or digital marketplace to be used*]. **Value for Money and Business Case** For each application moved to the cloud, a full business case will be developed to demonstrate compliance with this policy, and a full cost-benefit analysis will be developed, as well. These will cover: Benefit realization plans Total cost of ownership (TCO), inclusive of backups and disaster recovery requirements Value for money statement Identification of all associated integration requirements Discussion of the impact on information, privacy, people and process, as well as technology Should a major adoption of a cloud-based service be considered, the business case is expected to include an organizational skills assessment showing that the organization has the capability to manage the virtual service governance with appropriate contract management. **Probity** Cloud-based applications and systems are subject to the same internal audit standards as systems and applications hosted on-premises. Oversight committees will review (as part of their natural workload), the continuing effectiveness and efficiency of cloud arrangements, along with what may need amendments to comply with vendor terms and conditions. To this end, the adoption of common and open standards, where possible, is expected to ensure that the overall integrity and ease of integration with core systems is maintained. **Authorization** [*Insert organization's authorization process here*].

Scope/Limitations	State explicitly to whom this applies, such as departments, agencies or statutory bodies, and to whom it may not (such as arm's-length companies). **Example:** This policy applies to all government departments, statutory bodies and shared service providers. It does not apply to [*Organization Name*]-owned corporations; it is, however, recommended for adoption by those as well.
Compliance/Legislation	Outline what compliance requirements all those contracting cloud services are expected to abide by. This may include security, data protection and privacy, as well as any legislative requirement to host data within country. **Example:** The vendor is expected to comply with all specified security standards in line with security classification of the data. These are detailed here: [*Insert location of documents*]. Compliance with relevant or mandated third-party standards such as ISO/IEC 27001, HIPAA, FISMA are to be detailed within the business case for each application. The vendor must be obligated to immediately notify [*Organization Name*] of any security breach via the contractually agreed procedure. Failure to do so may result in penalties being levied in line with contractual terms and conditions. The vendor must prohibit unauthorized access to, use or alteration of, the data stored. The method and procedures for this must be detailed in the contractual terms. Legislation, for example, any Data Protection Acts that cover the provisions for the use and storage of personal and private data within a country/territory. Consider changing requirements, including the right to be forgotten, as enshrined in the forthcoming European General Data Protection Regulation.
Data Protection	Identify clearly any internal data protection requirements. **Example:** All existing internal information governance (IG) strategy controls and procedures must be adhered to and maintained. These can be found at [*Enter hyperlink to location of policy controls*]. Staff are expected to comply with these controls at all times when dealing with our data. Every department or staff member contracting any cloud service must report the details to a central register held by [*Enter location or department contact holding the register*], so that in the event of a problem with the service, or the contracting officer leaves the organization, we are aware of the service details. Our internal IT department [*Enter name*] will be expected to maintain the capability to monitor traffic flowing to and from our cloud service providers, and disciplinary action may be taken against those departments or individuals that are discovered to have failed to comply with the requirements of this policy [*Enter location of disciplinary policy*].
Data Management	Explicitly identify how data will be managed via a third party, if a hosting company (including IaaS and PaaS) is being used, or if SaaS is being considered. How will data be migrated/transported to the cloud provider? Identify the controls or checks to be implemented when data disposal is required at any point throughout, or at the end of the contract. Under what terms can the cloud provider have access to, or copy, the data? Identify the requirement for those contracting the service to ensure that adequate exit plans and funds are in place to recover the data quickly in an emergency and reprovision another system, or to tender for a replacement when longer exits are foreseeable. **Example:** All contracts must include explicit terms and conditions that include the fact that data ownership throughout resides with [*Organization Name*]. This policy calls for explicit exit plans for each application that is to be maintained in a central register. Any officer contracting a cloud-based service must update the register in the first instance. Two exit plans are required for every application or service used. The first exit plan required is application- and vendor-specific, and is invoked in the event of a catastrophic failure, such as: A significant security breach Vendor bankruptcy [*Add other criteria that could lead you to require the immediate return of data*] The second exit plan may be the single generic plan that is invoked for any application that is failing to perform adequately and is subject to early termination of the contract. In this situation and in end-of-contract termination, we can reasonably be expected to conduct another tendered procurement. All data uploaded to a cloud service by [*Enter name of organization*] or its users, citizens or partners must remain the property of [*Organization Name*] and may not be used without its written permission.
Data Access	Ensure the policy states the minimum required to ensure access to the data is maintained, especially in the event of some emergency event such as vendor bankruptcy. Ensure the contractual terms are clear that the [*Organization Name*] owns the data, including any associated metadata. **Example:** The cloud provider should, at all times, maintain accessibility to the data and, in the event of an enforced default, must provide [*Enter name of organization*] its data in an agreed format and time frame.

Risk Management	Clearly state the risk-based approach to using cloud-based services and any procedural requirements to be followed. **Example:** Agencies must undertake comprehensive risk assessments annually, and immediately following a significant issue, in relation to: Internal — network capability and resilience, privacy impact Vendor technical — penetration test to assess security risk Vendor viability The monitoring of the business health of our vendor community is important, as it can provide early warning signs of potential problems with any given vendor. This policy requires staff, contract owners and finance to work together to report and evaluate any emerging issues in line with our risk management policy. Failure to undertake the necessary assessments and inform relevant parties could result in disciplinary action.
Contact Information	This should be provided for escalation purposes when intended use may not exactly fit within the policy guidelines or where there may be clarification questions. Service desk as point of contact is a suggestion only. **Example:** For more information on this policy or to inquire about a variation that is not covered, contact the service desk by telephone [*Enter telephone extension number*] or email at [*Enter email address*].
Review Period	State by what date the policy is due to be reviewed. Early review is essential in such a fast-changing environment. Also, provide a feedback channel so that feedback to improve the policy is encouraged. **Example:** This policy will be reviewed annually or subsequent to any significant issue arising that has not been considered. Should you have any feedback (positive or negative), regarding the nature or operation of this policy, please inform [*Insert contact details, name, telephone number, email address for the appropriate mechanism*].
Other Standard Requirements	Section for normal policy elements such as document controls or glossary. Complete any existing organizational template requirements for document controls, related guidance, definitions, glossary and so forth.

FISMA = Federal Information Security Management Act (U.S.); HIPAA = Health Insurance Portability and Accountability Act (U.S.); IaaS = infrastructure as a service; ICT = information and communication technology; IEC = International Electrotechnical Commission; IG = information governance; ISO = International Organization for Standardization; PaaS = platform as a service; SaaS = software as a service; TCO = total cost of ownership

Source: Gartner (January 2017)

For more details, see "Government Cloud Use Policy Template" (https://www.gartner.com/document/code/302208?ref=grbody&refval=3582218)

Note 3
Five Key Questions for an Effective Cloud Computing Strategy

Source: "Devise an Effective Cloud Computing Strategy by Answering Five Key Questions." (https://www.gartner.com/document/code/270415?ref=grbody&refval=3582218)

The following questions need to be considered in preparation for creating any cloud strategy:

- Where and how will the enterprise consume cloud services?
- Where and how should the enterprise implement private cloud environments?
- How will we secure, manage and govern a hybrid IT environment?
- How will the enterprise's application strategy and architecture be impacted by cloud computing?
- Are there opportunities (requirements) for your organization to become a cloud service provider?

Note 4
Cloud Strategy Research for Technology Professionals

To support technology professionals working in roles such as the rapidly emerging cloud architect position, the Gartner for Technology Professionals service has published an extensive body of cloud research that includes the following:

- "2017 Planning Guide for Cloud Computing" (https://www.gartner.com/document/code/311457?ref=grbody&refval=3582218&latest=true)

"Solution Path for Developing a Public Cloud Strategy" (https://www.gartner.com/document/code/302159?ref=grbody&refval=3582218&latest=true)

"Designing a Cloud Strategy Document" (https://www.gartner.com/document/code/311458?ref=grbody&refval=3582218&latest=true)

"Decision Point for Application Placement: Cloud, Managed, Colocation or Do It Yourself" (https://www.gartner.com/document/code/270922?ref=grbody&refval=3582218&latest=true)

"Decision Point for Selecting an Application's Cloud Migration Strategy" (https://www.gartner.com/document/code/235074?ref=grbody&refval=3582218&latest=true)

"Analyzing the Role and Skills of the Cloud Architect" (https://www.gartner.com/document/code/317150?ref=grbody&refval=3582218&latest=true)

"The Cloud Architect's Guide to Implementing Public Cloud Services" (https://www.gartner.com/document/code/280976?ref=grbody&refval=3582218&latest=true)

"Key Services Differences Between AWS and Azure — Availability, Network, Compute and Storage" (https://www.gartner.com/document/code/301368?ref=grbody&refval=3582218&latest=true)

"Hybrid Architectures for Cloud Computing" (https://www.gartner.com/document/code/297323?ref=grbody&refval=3582218&latest=true)

"Building an IT Business Case for Public Cloud IaaS or PaaS" (https://www.gartner.com/document/code/292471?ref=grbody&refval=3582218&latest=true)

"A Comprehensive List of Management Requirements for Organizations Using Public Cloud Services" (https://www.gartner.com/document/code/276381?ref=grbody&refval=3582218&latest=true)

"Hosted Private Clouds: The Alternative to Building It Yourself" (https://www.gartner.com/document/code/292932?ref=grbody&refval=3582218&latest=true)

"Evaluation Criteria for Cloud Infrastructure as a Service" (https://www.gartner.com/document/code/301365?ref=grbody&refval=3582218&latest=true)

"In-Depth Assessment of Amazon Web Services" (https://www.gartner.com/document/code/301366?ref=grbody&refval=3582218&latest=true)

"In-Depth Assessment of Microsoft Azure IaaS" (https://www.gartner.com/document/code/301367?ref=grbody&refval=3582218&latest=true)

"In-Depth Assessment of Google Cloud Platform" (https://www.gartner.com/document/code/307694?ref=grbody&refval=3582218&latest=true)

The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity. (https://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp) "