Gartner Licensed for Distribution

The Cloud Strategy Cookbook, 2019

Published 2 April 2019 - ID G00385759 - 20 min read

By Analysts David Smith

Every business can benefit from a cookbook approach to developing a cloud strategy. CIOs should focus efforts on a living document that connects business strategy to implementation and migration plans.

Overview

Key Findings

- The top questions in cloud computing today revolve around cloud strategy. They are becoming more urgent and range from “What is a cloud strategy and why do I need one” to “How do we build a comprehensive cloud strategy?”
- Cloud strategy formulation leads to many secondary questions around principles and prioritization. These questions must be aligned with other strategies.
- One of the most important, and usually missing, components of a cloud strategy is an exit strategy.

Recommendations

As a CIO building a cloud computing strategy, you should:

- Build a cloud strategy in a short, living document that should be a concise point of view on the role of cloud in your organization. Cloud strategy does not equate to moving everything to the cloud.
- Ensure that your cloud strategy aligns with other strategic plans (for example, data center, security and architecture) and provides guidance to adoption plans.
- Plan for the cloud strategy to be the launching point for all the subsequent cloud activities: architecture, assessment, migration, operations, etc.
- Include an exit strategy that defines how you will get out of a particular cloud decision in the event it doesn’t work out as planned. An exit strategy is very important, even though you may never use it.

Analysis

This document was revised on 22 May 2019. The document you are viewing is the corrected version. For more information, see the Corrections (http://www.gartner.com/technology/about/policies/current_corrections.jsp) page on gartner.com.

A cloud strategy is a concise viewpoint on the role of cloud computing in an organization.

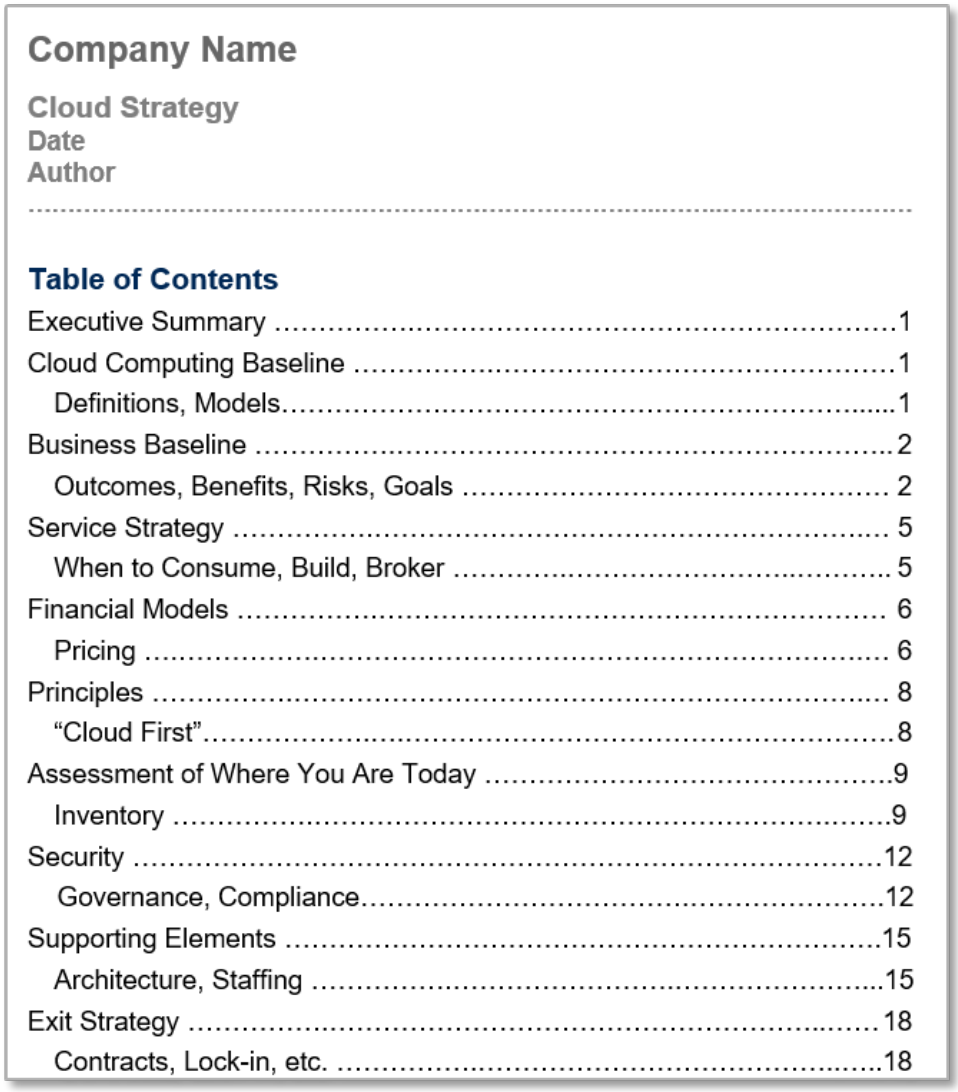
This research, in conjunction with a companion document "Formulate a Cloud Strategy in the Context of Your Overall Strategy," forms a comprehensive view of cloud strategy.

Organizations with a cloud strategy have more coherent approaches to cloud usage, anticipating both the benefits and potential downsides of cloud use, attempting to maximize the former while minimizing the latter. We see better outcomes with those that have a strategy than with those that do not. The various subdisciplines — procurement, sourcing, coding, infrastructure and operations (I&O), security, etc. — cannot be fully prepared to meet the organization's needs if they don't have a common strategy to draw on, and to look to for their priorities.

The cloud strategy cookbook is a virtual template. Based on reviews and discussions with hundreds of clients, it is what we would consider best practices for building a cloud strategy. A high-level overview of the main sections starts with an executive summary. We go through some baselines and things that might be considered the "meat," such as principles and an assessment of where you are today. Figure 1 represents a high-level outline of such a document.

Figure 1. Outline for a Cloud Strategy Cookbook

Outline for a Cloud Strategy Cookbook



Company Name

Cloud Strategy
Date
Author

Table of Contents

ID: 385759

© 2019 Gartner, Inc.

Source: Gartner (April 2019)

The top questions in cloud computing today revolve around cloud strategy. While these questions have evolved, they continue to be top of mind and are becoming more urgent. They range from "What is a cloud strategy and why do I need one" to "How do we build a comprehensive cloud strategy?" Such questions lead to secondary ones around principles and prioritization. Also, they must be aligned with other strategies (for example, data center, security, architecture).

CIOs and IT leaders struggle with prioritization and creating a strategy to ensure cloud success. This research provides actionable advice on structuring a cloud strategy document and principles to guide you, while offering guidance on determining which applications go where. We follow a "cookbook approach" to building a cloud strategy, utilizing principles such as bimodal IT.

Some details on the sections begin with the first page of the cookbook (see Figure 2).

Figure 2. Cloud Strategy Cookbook Template Details

Cloud Strategy Cookbook Template Details

- **Executive Summary:**
  - Summary of drivers, challenges and major steps
  - Cloud council members, roles, org.
- **Cloud Computing Baseline:**
  - Cloud-defined (attributes, service categories, delivery models) — don't reinvent this. Use NIST, Gartner Cloud Spectrum
  - Delivery models (public, private, hybrid, multi ...)
  - Adoption statistics
  - **Action:** Training and communications plan
- **Business Baseline:**
  - Desired business outcome targets
  - Potential benefits — generic, bimodal-driven
  - Potential risks (generic — e.g., security, compliance)
  - Other factors (e.g., data center strategy), unique issues to your business in your industry in your geography at this time
  - **Action:** Map potential benefits to desired business outcomes while overcoming challenges/risks

ID: 385759 © 2019 Gartner, Inc.

Source: Gartner (April 2019)

Executive Summary

An executive summary is for people who don't get beyond the first page. So it should summarize what the document says. This is also the place to put the names and organizations of the people in your cloud council. If you do the strategy right and have members from all the different roles, it makes a very big statement that this is not just an IT document. Writing this section last makes sense, as it summarizes the entire effort.

Cloud Computing Baseline

This should be simple. The U.S. National Institute of Standards and Technology (NIST) has come up with a set of definitions, as has Gartner (see "NIST and Gartner Cloud Approaches Are More Similar Than Different"). While NIST's definition is not perfect, it is important because with it, you can eliminate the majority of disagreements with people so they're at least on the same page regarding what the terminology means. There are further definitions, including hybrid and multicloud, and pure cloud and cloud-inspired (described in Gartner's Cloud Spectrum; see "Four Types of Cloud Computing Define a Spectrum of Cloud Value"). Leverage, don't reinvent, here. This section can also point to details in an appendix.

Note that it is much less important what the definitions are than the fact that you have them and agree to them. The key is to eliminate confusion within the organization by agreeing to the definitions and then using them consistently when talking about cloud.

The output from this effort is to populate a training and communication plan, which is essential to broadening the discussions around cloud.

Business Baseline

This section should summarize the top-level business strategy and desired business outcome targets, as well as business transformation initiatives. Those should be coming from the company's top-level strategy. The next step is to look at the potential benefits and potential risks. These are mostly generic and aligned with bimodal IT principles (see "Your Cloud Strategy Needs to Be Bimodal").

This means knowing what the goals are (typically either cost cutting/cost-efficiency [Mode 1]) or agility/innovation (Mode 2) and considering the potential ways that cloud can help achieve those goals. Then examine things that are unique to your organization. What is your business trying to accomplish in your industry, in your geography, at this point in time? Is there a data center strategy that you need to make sure that you are aligning with? Are there extenuating circumstances?

The action is to map the business goals to the potential benefits of cloud and overcome the potential challenges. This section should state why the organization is interested in cloud in the first place.

The next set of details is shown in Figure 3.

Figure 3. Cloud Strategy Cookbook Template Details (Continued)

Cloud Strategy Cookbook Template Details (Continued)

- **Service Strategy:**
  - When to consume
  - When to build
  - When to be a broker — hybrid IT operating model
  - How to secure/manage/govern hybrid environments
  - Becoming a provider?
  - **Action:** Examine all roles in cloud
- **Financial:**
  - Pricing
  - Chargeback
  - Payment models
  - Capex vs. opex
  - **Action:** Ensure understanding of all options

ID: 385759

© 2019 Gartner, Inc.

Source: Gartner (April 2019)

Service Strategy

Determining your service strategy is done by deciding when you would be consuming cloud services from a public cloud provider versus when you will build (or at least continue to maintain capabilities on-premises elsewhere). Distinguishing between use cases for infrastructure as a service (IaaS), platform as a service (PaaS) and SaaS should be part of this discussion. This is also where to address scenarios when you would want to be a broker, and how to have a hybrid IT operating model where you are simultaneously consuming services, being the middleman and providing services yourselves. A question to ask includes, “How do you secure, manage and govern the resulting hybrid environment?” It is important to acknowledge that virtually all enterprises are hybrid because almost no company of any size today can afford to do everything itself or put everything in a public cloud.

Deciding to build actual cloud services is not a decision to be made lightly. Trying to do so is a large effort. Most organizations will maintain some on-premises capabilities but not try to duplicate the functionality of hyperscale cloud providers.

The action here is to examine the applicability of all potential roles in cloud — consumer, provider and broker.

Financial

It is imperative to understand the financial implications of cloud at a high level. Its importance is why we say involving finance professionals matters, because they understand things that most IT professionals do not spend a lot of time thinking about. Issues regarding cost transparency, visibility, budgeting and predictability should be considered. Cloud typically is funded by an operating expense model instead of a capital expense model. However, there are companies where owning capital assets is a key part of the corporate strategy; thus, if you change everything to an operating expense, It could change the financial profile of the organization. We have seen many examples of this occurring unintentionally.

Understanding the trends around the pricing models is important to ensure that expectations are met. For infrastructure as a service, since it's mostly aligned with hardware costs, the price tends to go down slowly over time. With IaaS, it's primarily a pay-as-you-go model where contracts are not required, but may be desirable in some scenarios (such as for pricing discounts). Contrast that with the model in SaaS for applications where the prevalent model is subscription — typically a three-year contract, per user per month — and that price tends to go up over time. It is also critically important to avoid succumbing to myths such as you always save money moving to the cloud (see "The Top 10 Cloud Myths").

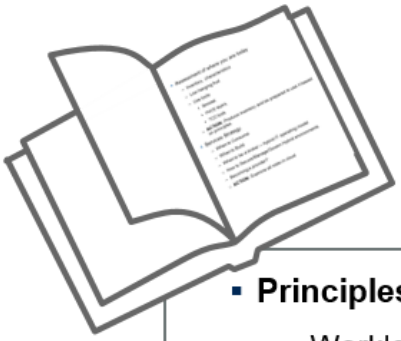
The action is to ensure an understanding of the many implications of the financial options available. This is not a business case either for or against cloud.

Principles and Assessment/Inventory of Where You Are Today

Principles and assessment/inventory of where you are today are, in many ways, the meat of a cloud strategy. They are described in more detail in Figure 4.

Figure 4. Cloud Strategy Cookbook Template Details (Continued)

Cloud Strategy Cookbook Template Details (Continued)



- **Principles:**
  - Workload by workload (nonnegotiable)
  - Potential principles:
    - Cloud-first
    - Buy before build (SaaS-first in cloud terms)
    - Best of breed
    - Multicloud, cloud-native
  - Lift-and-shift last resort
  - Vendor considerations
  - **Action:** Validate
- **Assessment of where you are today:**
  - Inventory, characteristics
  - Use tools:
    - Bimodal
    - Pace layers
    - TCO tools
  - **Action:** Produce inventory and be prepared to use it based on principles

ID: 385759 © 2019 Gartner, Inc.

Source: Gartner (April 2019)

Principles

There are many potential principles that can determine a cloud strategy. Some are nonnegotiable — for example, a cloud strategy is a workload-by-workload or application-by-application exercise (workloads are groupings of applications). Some other principles, such as "Lift-and-shift migrations to public cloud should be a last resort" are recommended and should be explicitly stated. You generally don't get a lot of benefits from doing lift-and-shift migrations. It doesn't mean you don't ever do it. Sometimes it makes a lot of sense to do it; for example, if you have a data center strategy for consolidation, you have to find a home for things. But don't expect to get a lot of cost savings or agility benefits from lift and shift. It may make sense for other reasons, such as when you don't want to change the application (to avoid potential disruptions in operations) and the application needs to be colocated with data or applications that have been moved to cloud (for all the right reasons). Using lift and shift just to move the application to cloud rarely makes sense.

There may also be vendor-oriented considerations that you want to document as well, be they for positive relationships or investment in skills, etc.

Some common principles are:

- Cloud first
- Buy before build (which, in the cloud, is often stated as SaaS first)
- Best of breed

There may also be architectural principles such as cloud-native or multicloud. These issues are also often addressed in the exit strategy or in aligning with architectural principle documents.

Cloud first is a very common principle guiding cloud strategies and adoption decisions. Some people dismiss it as a slogan. It's more than that, but It's not a whole strategy. Cloud first doesn't mean everything goes to the cloud. It means that, when you ask for an investment (for example, when you want to renew something, enhance something or build something), the preferred approach is to use public cloud. It also means that any new technology or business initiative should consider cloud as the first option. It doesn't mean that in all cases it will be public cloud, but it's the default that you work back from. Start with the assumption that, unless there's a reason not to, you go with public cloud, and then you back off as necessary. Cloud first is the recommended approach in most cases from Gartner. It's not reasonable when people place enormous burdens when putting things in the cloud or not putting things in cloud. You want to do the right thing for the particular workload.

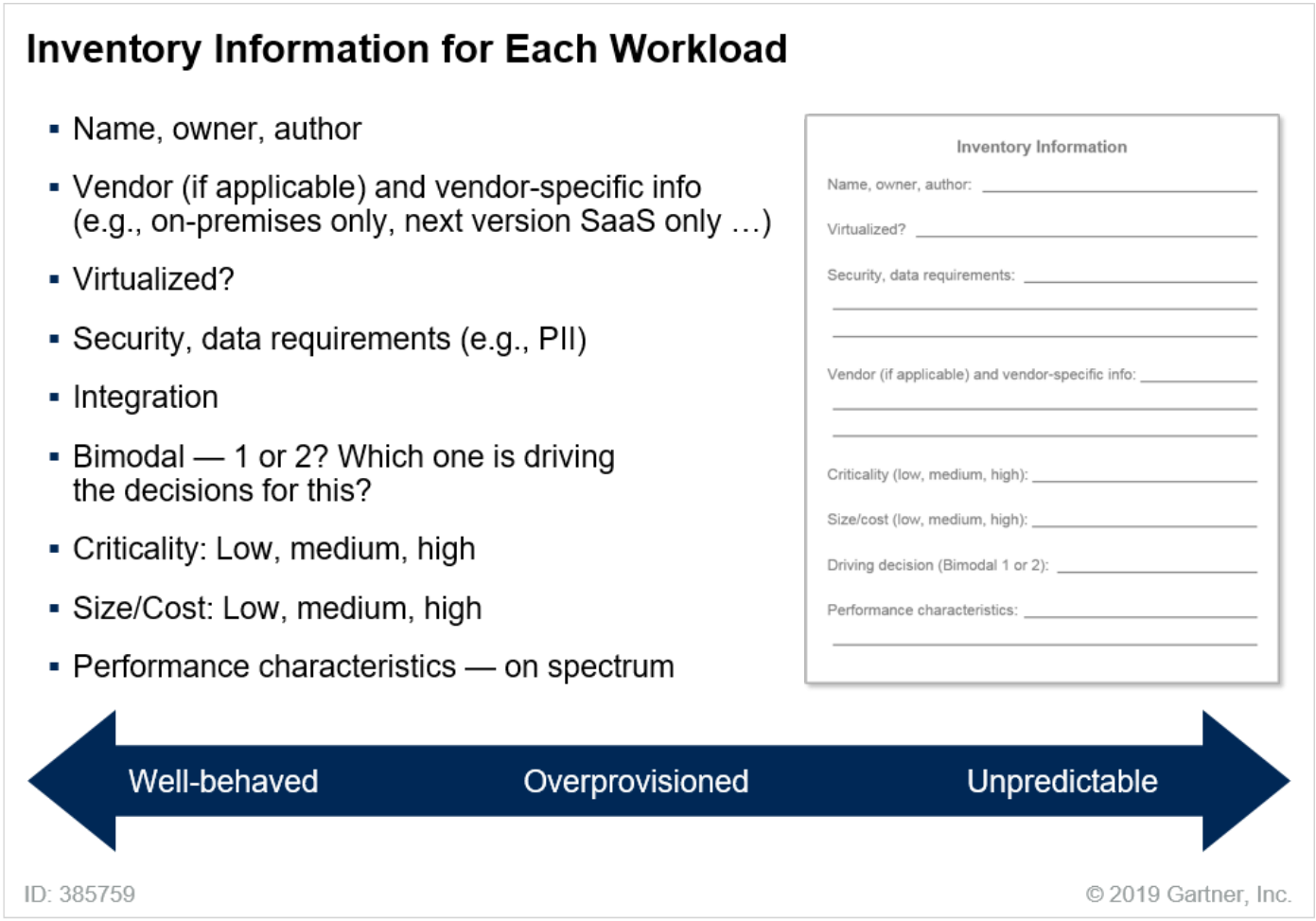
Assessment of Where You Are Today — The Inventory

As a cloud strategy should be applied workload by workload, an inventory of those workloads is warranted. Simply, a workload is a collection of applications that belong together. For each workload, you want to have a set of information at your fingertips.

What kinds of information would be useful for you to capture about each of those workloads to make decisions about them? Gartner concepts and tools such as bimodal IT can help here. This concept is applicable not just at a high level, but also for each workload. Is the goal to save money on this application? Is the goal to be more agile? If the goal is to be more agile, it may cost more, and that may well be acceptable. Other tools such as total cost of ownership (TCO) and pace layering (see "Pace-Layered Application Strategy and Organizational Design: How to Structure the Application Team for Success") can be very helpful.

The effort of collecting this information is often shared between the strategy phase and the implementation phase. The strategy phase should include determining the scope and starting the effort. Figure 5 shows the elements of an inventory.

Figure 5. Inventory Information



Source: Gartner (April 2019)

There is some basic information that you need to have. What's the name of the workload? Who owns it? Who authored it (if you wrote it yourself in-house)? Are there dependencies on other applications? Is there a vendor involved? Is it a packaged application from a vendor? Are there things you should know about that (for example, you could be on the last on-premises version from this vendor and if you want to upgrade, then you have to go to its SaaS version)?

Is it virtualized? What are the security, governance, compliance and data requirements? Does it have PII and security requirements? Special integration requirements or location requirements? What's the goal here? What's driving the decisions? Is this a cost savings efficiency decision or is this more of an agility decision?

If you're like most organizations, you're going to find hundreds, if not thousands, of workloads that you have to go through. The actual effort of going through those is often left to the implementation and adoption phase. You may find applications that people might not even be running, in which case there may be opportunities to turn them off. It is important to look for the important ones to focus on — the most critical workloads and those that are costing the most. These are the ones to focus on and understand well before you make a big decision around any changes.

Performance characteristics are an important factor. This is where you look at whether you have something that is a particularly good candidate for cloud. Utilizing a spectrum is helpful. On one end of the spectrum, you have an unpredictable workload — like a website, a mobile app

or an API gateway — something that is externally facing and for which it is difficult or impossible to predict what the demand will be. On the other end of the spectrum, you have well-behaved applications. This is a typical enterprise application that is already virtualized and running efficiently in your data center. It's a steady-state type of application that doesn't vary much and doesn't have peak workloads. It's very predictable. That is the opposite of an unpredictable workload and one that does not benefit from typical cloud characteristics.

If an application works and it's cost-effective, it should not be a high priority to change. However, extenuating circumstances (such as a data center strategy that is to close the data center) may force action. In the middle of the spectrum, there are shades of gray; for example, you have the classic overprovisioned workload (such as a certain baseline) and, at the end of the month or the holiday season, you have a peak and have to overprovision for it. These are decent candidates to consider for going to the cloud.

Security

Security warrants a statement or two on its own because it's so important. Attitudes toward security vary, but we have seen a big change. Until a few years ago, the conventional wisdom was that public cloud is not secure enough today. Now, we're in danger of going to the opposite extreme where organizations sometimes trust public cloud providers too much.

"Clouds Are Secure — Are You Using Them Securely?" recommends focusing on understanding the roles in security properly. While the top-tier cloud providers do an excellent job of securing the services they provide (for example, Amazon Web Services [AWS] secures the services — IaaS — that include virtual machines, storage and networking), they do not secure the applications or data that you host there. You are responsible for making sure that the data you put on IaaS is locked down appropriately. It's not the provider's fault if you leave your data unprotected. Identifying responsibilities is critical to secure use of the cloud.

Security Is a Great Example of the Importance of Alignment With Other Strategies

The right way to approach security and all these other supporting elements, such as technical architecture, infrastructure, staffing and procurement, is to ensure that they are in alignment. Figure 6 describes these. If you need to put something about security in the cloud strategy, make sure it also goes in your security strategy and vice versa, and that it is aligned. Sometimes that may mean modifying the overall security strategy.

Figure 6. Cloud Strategy Cookbook Template Details (Continued)

Cloud Strategy Cookbook Template Details (Continued)

- **Security:**
  - State security principles
  - Identify responsibilities
  - Governance, compliance
  - Incorporate principles from security strategy
  - **Action:** Apply result to security strategy and cloud strategy
- **Supporting Elements:**
  - Current business and technical architecture and infrastructure
  - Staffing issues
  - Alignment with other strategy, efforts
  - **Action:** Update other strategies — security, etc.
- **Exit Strategy:**
  - Contracts with T&C, SLA
  - Data ownership, backup, getting data back
  - Lock-in, etc.
  - By type of service
  - Development/architectural issues
  - Multicloud strategies
  - **Action:** Don't forget the exit strategy!

ID: 385759 © 2019 Gartner, Inc.

Source: Gartner (April 2019)

The right way to approach security is to have high standards and to utilize concepts like tiering of providers. There is a long tail — top tiers like AWS and Salesforce that do an excellent job at security. But anyone can claim to be a cloud provider and may not have anywhere near the same level of security capability as a top-tier provider. Also, it is very important to identify responsibilities in cloud security.

Anything that's in your existing security strategy needs to be adhered to or changed to accommodate the realities of cloud.

While not security per se, issues such as governance and compliance are often grouped in the topic. Alignment with existing strategies, as well as processes specific to cloud, should be addressed here as well, although these topics are often included in implementation plans.

Supporting Elements — Organizational and Staffing Issues

As with the aligning of cloud security issues with an overall security strategy, a similar approach should also be taken when it comes to staffing. Cloud changes staffing requirements, depending on what level of cloud service you're interacting with. You will need different mixes

of skill sets. You will likely need fewer people who manage servers directly, but more people who do higher-level tasks like integration, network engineering, business analysis, vendor management, security, etc. It's not just position reduction; there are also growth opportunities for some and it's important to have the right people involved. That's why including HR in this effort makes sense.

The cloud strategy council and cloud center of excellence constructs also warrant discussion from an organizational perspective.

Exit Strategy

One of the last pieces, but most important, is an exit strategy. An exit strategy defines how you will get out of a particular cloud decision in the event it doesn't work out as planned. Even for those that have a cloud strategy, most don't typically have an exit strategy. An exit strategy is very important, even though you may never use it. Cloud repatriation (moving of workloads back from public cloud) is rare. However, awareness and planning regarding possibilities is an important part of strategic planning. Several regulators, primarily in the EU and focused on financial services, are now mandating an exit strategy.

Those who do look at exit strategies often look mostly at contracts — terms and conditions, service-level agreements, etc.; basically, how to get *out* of a contract. That's important, but it's just the beginning when it comes to exit strategy. You also have to look at data ownership, backup, getting your data back, portability, etc. The exit strategy should include technical factors *and* business factors. Sometimes the hardest part about leaving a cloud service is the contract, not the technology. And don't forget all the supporting infrastructure for the cloud service, including networking, management tools, integration and third-party services.

Lock-in is one of the main issues that should be discussed as part of an exit strategy. There are many different places you can have lock-in: at the data level, the application level, the architecture level or the skills level. This is often the impetus to start you down the path of looking at multicloud strategies. Multicloud is one of the great buzzwords today.

Many say they want multicloud but, at the same time, note in their cloud strategy documents that they also want to be cloud-native. These are not necessarily completely at odds with each other, but if you take them to their logical extremes, they can be. If you want to be completely multicloud and not dependent on a vendor, then you can't take advantage of all of the native capabilities of that vendor. There are trade-offs. It's not a simple answer, but the cloud strategy is where this should be handled.

A common progression occurs as enterprises get more mature in their use of cloud. They'll usually start off with a few projects with one provider. After initial successes, before long they have many workloads there and a corresponding large invoice, and they begin to worry that they're too dependent on one vendor. As a result, they'll start down the path of a procurement-driven multicloud strategy looking to encourage competition. After that, they start looking at a management strategy where they want a single pane of glass for monitoring. Eventually, some

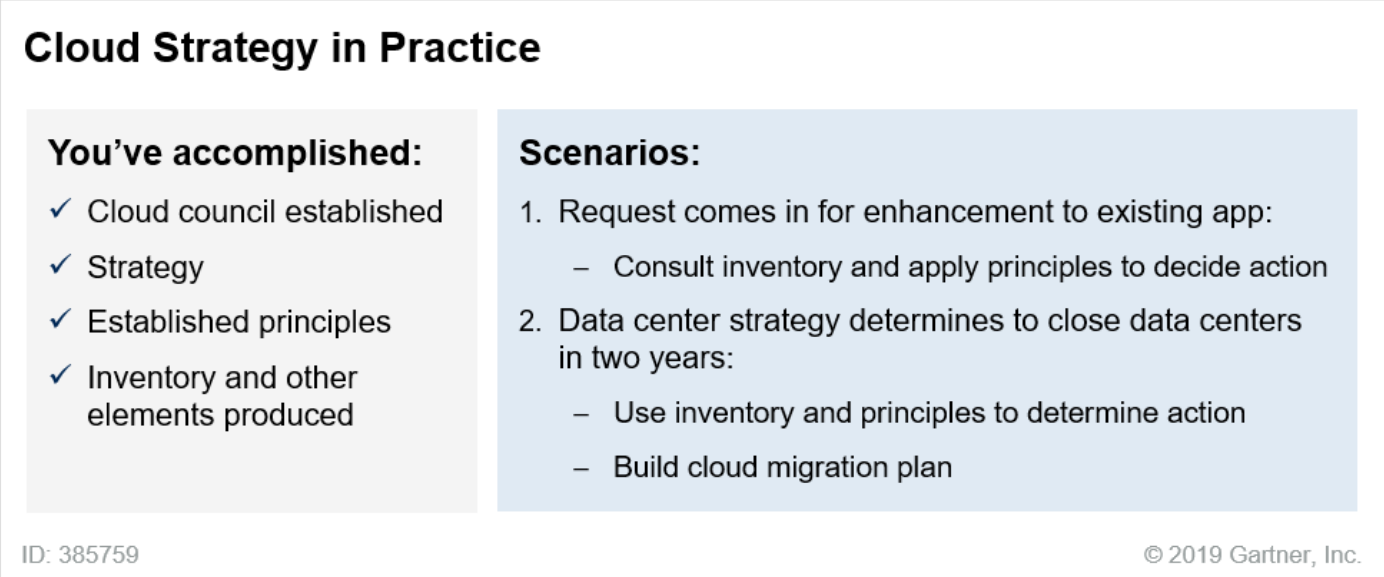
get to the architectural part, focusing on portability of applications and the role of technologies such as containers, PaaS and open source.

So don't forget the exit strategy. It really is important.

Cloud Strategy In Practice

In practice, the cloud strategy works as follows (see Figure 7). You have established your cloud council, produced your cloud strategy and established your principles. You have also at least started down the path of producing the inventory.

Figure 7. Cloud Strategy in Practice



Source: Gartner (April 2019)

If you have determined that your strategy will follow a cloud-first principle, then it works as follows: When a request comes in for an enhancement to an existing application, you consult the inventory and you apply the principles to each request. It gets more complicated if there's a data center strategy that says you're going to close the data centers in two years. If that happens, you have to start to build a cloud migration plan in which you have to find homes for everything. Unless you have that kind of an edict, there is no reason to go through all your applications and move them.

This is where the connection with a data center strategy comes in, and where you move from strategy to execution. This is where you look at best practices, lessons learned and ways to efficiently migrate hundreds of applications to the cloud, if that makes sense. While data center and I&O-centric views often drive the extenuating circumstances, there are other considerations such as application modernization, M&A, new product development, business resilience and other strategies that may trigger mass migrations.

On to the Implementation/Adoption/Migration Phase

A cloud strategy is a living document. As such, it feeds the next phase of implementation. Beyond cloud strategy is implementation (also referred to as adoption or migration).

There is a great deal of Gartner research to assist with the implementation phase, including:

- “A High-Level Framework for Planning Your Migration to Public Cloud Services”
- “How to Begin Using Public Cloud Infrastructure as a Service”
- “2019 Planning Guide for Cloud Computing”
- “Moving Enterprise Workloads to Public Cloud, Hosting or Colocation — How to Prioritize and Execute”

© 2019 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While 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. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner’s Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."

© 2018 Gartner, Inc. and/or its Affiliates. All Rights Reserved.