The Cloud Strategy Cookbook, 2021

Published 17 February 2021 - ID G00741474 - 19 min read

By Analysts David Smith

Initiatives: Cloud and Edge Infrastructure

Organizations that create a cloud strategy gain the most from their use of cloud computing. Infrastructure and operations leaders should use our cookbook approach to creating a “living” cloud strategy document that connects business strategy to implementation and migration plans.

Overview

Key Findings

- Many organizations lack a cloud strategy. They don't achieve as much from their use of cloud computing as organizations with a cloud strategy.

- Devising a cloud strategy leads to many secondary questions about principles and prioritization. Effective cloud strategies align these questions with other strategies.

- A cloud strategy is different from a cloud implementation plan. A cloud strategy answers the “what” and “why” questions, while a cloud implementation plan answers the “how” questions.

- An exit strategy is one of the most important components of a cloud strategy, but it's often missing.

Recommendations

Infrastructure and operations leaders responsible for cloud strategy as part of their cloud and edge infrastructure:

- Maximize the benefits from your use of cloud computing by creating a cloud strategy. Make it a living document that provides a concise view on the role of cloud computing in your organization.

- Align your cloud strategy with other strategic plans (for example, those for data center, security and architecture). Do so by communicating and negotiating with all stakeholders.

- Plan for your cloud strategy to be the launching point for all subsequent cloud activities, such as architecture, assessment, migration and operations. Achieve this by keeping those activities in mind when devising your cloud strategy.
Gain More From the Cloud With a Cloud Strategy

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

Organizations with a cloud strategy are in a better position to achieve better outcomes from cloud computing than those without one. They have more coherent approaches to cloud usage. They anticipate both the benefits and potential downsides of cloud use, attempting to exploit the benefits while minimizing the downsides. As an I&O leader, you can’t be fully prepared to meet your organization’s needs if you don’t have a common strategy to draw on, and to consult for priorities, along with your colleagues in the other subdisciplines of IT.

Many of the top questions in cloud computing revolve around cloud strategy. And these questions 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 others about principles and prioritization. Also, you must align your cloud strategies with other strategies (for example, data center, security and architecture strategies). Your organization’s cloud strategy should enable its digital transformation initiatives.

Although it’s best to craft a cloud strategy before adopting cloud computing, that’s rare. Most organizations devise their cloud strategy after they’ve gained some experience with the cloud. But the sooner you establish a cloud strategy, the more issues you’ll avoid. It’s never too late to develop a cloud strategy. If you don’t have one already, today’s the best time to start creating one.

Use this research, along with Align Your Cloud Strategy With the Organizational Strategic Plans and Top 10 Tips for Avoiding the Most Common Mistakes in Cloud Strategies, to devise a sound cloud strategy.

Use Our Cookbook as a Template

Our “Cloud Strategy Cookbook” provides a virtual template. We’ve based it on reviews and discussions with hundreds of clients. Creating a cloud strategy following our cookbook is a best practice. An executive summary gives a high-level overview of the main sections. The strategy should then include some baselines and, perhaps the most important elements, the principles and an assessment of your current position. Figure 1 shows a high-level outline of a cloud strategy.
Outline for a Cloud Strategy Document

Start by using the Cloud Strategy Council construct (described in Align Your Cloud Strategy With the Organizational Strategic Plans). Note the differences between a cloud strategy document (which is the focus of this approach), and a cloud adoption or migration plan. The strategy document answers “what” and “why” questions, while an adoption/migration plan addresses “how” questions.

The first page of the document gives some details of the executive summary and the baselines (see Figure 2).
Executive Summary

The executive summary is your chance to communicate with senior management. Use it to summarize the document. Include the names and organizations of the people in your cloud council (described in *Align Your Cloud Strategy With the Organizational Strategic Plans*). Include people in all the different roles to show that your cloud strategy is not just an IT document. Write the executive summary last because it summarizes the entire effort.

Baselines

Establish an effective cloud strategy by creating baselines for cloud computing and the desired business outcomes.

Cloud Computing Baseline
Keep this simple. The U.S. National Institute of Standards and Technology (NIST) has drawn up a set of definitions, as have we (see NIST and Gartner Cloud Approaches Are More Similar Than Different). No definitions are perfect, but they enable you to eliminate most disagreements because people at least agree what the terminology means.

Many newer terms in cloud computing (for example, cloud native, multicloud and distributed cloud) are often cited as core parts (even principles) of a cloud strategy. But the meanings of such terms aren’t well established. If you use them, clarify their meaning (see Define and Understand New Cloud Terms to Succeed in the New Cloud Era). You may want to use other terms such as pure cloud and cloud-inspired (described in Gartner’s Cloud Spectrum; see Four Types of Cloud Computing Define a Spectrum of Cloud Value) to provide clarity. Use existing terms, don’t reinvent them. In this section you can also refer to an appendix that gives more details.

What’s important is that you agree on the definitions. The key is to eliminate confusion by agreeing on the definitions and using them consistently when talking about cloud computing.

Creating a cloud strategy will enable you to populate a training and communication plan, which is essential to broadening discussions about the cloud.

Business Baseline
In this section, summarize the top-level business strategy and desired business outcomes, as well as business transformation initiatives. Use annual reports, speeches by senior management and conversations with business leaders as sources.

Next, look at the potential benefits and risks. These are mostly generic and aligned with bimodal IT principles. You must know what the goals are (typically cost cutting/cost-efficiency or agility/innovation), and assess the ways in which cloud computing can help achieve those goals. Then examine issues unique to your organization. For example, explore:

- What your business is trying to accomplish in your industry, in your region
- Whether you need to align with a data center strategy
- Whether extenuating circumstances exist
- The impact of responding to uncertainties such as the pandemic

This section should map the business goals to the potential benefits of cloud computing and explain how to overcome the potential challenges. It should state why the organization is interested in the cloud.

Brainstorming
Services strategy, financial considerations and other considerations make good discussion points when brainstorming the main principles that will drive your cloud strategy. Documenting these will increase
your understanding of those principles and how to use them (see Figure 3).

**Figure 3. Cloud Strategy Document — Brainstorming**

**Cloud Strategy Document — Brainstorming**

The Cloud Strategy Document

<table>
<thead>
<tr>
<th>Services Strategy</th>
<th>Financial:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• When to consume</td>
<td>• Address cost myths</td>
</tr>
<tr>
<td>• When to build</td>
<td>• Pricing</td>
</tr>
<tr>
<td>• When to be a broker — hybrid IT operating model</td>
<td>• Chargeback</td>
</tr>
<tr>
<td>• How to secure/manage/govern hybrid environments</td>
<td>• Payment models</td>
</tr>
<tr>
<td>• Becoming a provider?</td>
<td>• Capex vs. opex</td>
</tr>
</tbody>
</table>

**Action:** Examine all roles in cloud

Source: Gartner
741474_C

**Services Strategy**

Determine your services strategy by deciding when you would consume cloud services from a public cloud provider and when you will build — or at least continue to maintain — capabilities on-premises or elsewhere. Distinguish between use cases for infrastructure as a service (IaaS), platform as a service (PaaS) and SaaS. Address scenarios in which you may want to be a broker, and how to have a hybrid IT operating model in which you simultaneously consume services, act as a middleman and provide services. Ask, “How do we secure, manage and govern the resulting hybrid environment?” Note that virtually all enterprises are hybrid because almost no company (except startups) can afford to do everything itself or put everything in a public cloud.

Don’t take the decision to build cloud services lightly. It’s a huge effort. Most organizations maintain some on-premises capabilities but don’t try to duplicate the functionality of hyperscale cloud providers.
Examine the applicability of all potential roles in cloud computing — consumer, provider and broker (including governance).

**Financial Considerations**

You must understand, at a high level, the financial implications of cloud computing. Involve finance professionals because they understand the implications of changes to corporate financial models. Examine issues such as cost transparency, visibility, budgeting and predictability. Organizations typically fund cloud computing from operating expenditure rather than capital expenditure. However, owning capital assets is a key part of the corporate strategy for some companies. If you change everything to an operating expense, it could change your organization's financial profile.

Understand pricing model trends to ensure that you meet expectations. For example, IaaS is mostly aligned with hardware costs, so the price tends to go down slowly over time. IaaS is mainly a pay-as-you-go model. Contracts aren’t required for IaaS, but may be desirable in some scenarios (such as for pricing discounts). Contrast that with SaaS for applications where the prevalent model is subscription. SaaS contracts are typically three years and per user per month. The price for SaaS tends to go up over time. And above all, don’t believe the biggest myth about the cloud — that you always save money by moving to it (see [Revisiting the Top 10 Cloud Myths for 2020](#)).

Completing this section of the cloud strategy will give you an understanding of the many implications of the financial options available. It is not intended to give you a business case either for or against cloud computing.

**Principles and Inventory (Assessment of Current Position)**

The principles and inventory (assessment of current position; see Figure 4) are, in many ways, the most important parts of a cloud strategy.
Principles

Many principles can determine a cloud strategy. Some are non-negotiable — for example, a cloud strategy is a workload-by-workload or application-by-application exercise (workloads are groupings of applications). Others, such as “lift-and-shift migrations to the public cloud should be a last resort,” are recommended and should be explicitly stated.

You generally don’t gain much from lift-and-shift migrations. Although sometimes lift and shift makes sense; for example, if you have a data center strategy that states data center closure is the goal, you need to align with it, which often means you have to find a home for things. But don’t expect to get huge cost savings or gain many agility benefits from lift and shift. Such a migration 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 must be colocated with data or applications that have been moved to the cloud (for all the right reasons). But using lift and shift just to move the application to the cloud rarely makes sense.
Also document any vendor-oriented considerations, such as positive relationships or investment in skills.

Some common principles are:

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

Some of these may be architectural principles, such as cloud-native or multicloud. You may want to address these issues in your exit strategy or when aligning with architectural principle documents.

Cloud first is a common principle guiding cloud strategies and adoption decisions. Some people dismiss it as a slogan. Although it’s more than that, 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, enhance or build something), the preferred approach is to use public cloud.

Cloud first also means you should consider the cloud as the first option for any new technology or business initiative. We recommend cloud first in most cases. Do the right thing for the particular workload.

**The Inventory (An Assessment of Current Position)**

As your cloud strategy is workload by workload, you must inventory those workloads. For each workload, you must have a set of information at your fingertips.

Gartner concepts and tools such as bimodal IT can help you decide what kinds of information would be useful to capture about each workload to help you make decisions. Is your goal to save money on this application? Is your goal to be more agile? If your goal is to be more agile, it may cost more, and that may be acceptable. Other tools such as total cost of ownership and pace layering can be helpful.

You will probably collect this information in the strategy and implementation phases. Determine the scope and start the effort in the strategy phase. Figure 5 shows the elements of an inventory.
You must include some basic information for each workload, including answers to the following questions:

- What's the name of the workload?
- Who owns it?
- Who authored it (if you wrote it in-house)?
- Does it have dependencies on other applications?
- Is a vendor involved?
- Is it a packaged application from a vendor?
You'll probably have hundreds, if not thousands, of workloads to examine. You may leave the work of going through them to the implementation and adoption phase (or a separate project). Your organization may not even use some of the applications, in which case you may be able to turn some of them off. Focus on the most critical workloads and those that are costing the most. Understand them thoroughly before you make big decisions about changes.

Performance characteristics are important when deciding whether you have a good candidate for the cloud. Using a spectrum is helpful. On one end of the spectrum, you have unpredictable workloads. These are externally facing and difficult or impossible to predict demand for, such as a website, a mobile app or an API gateway. On the other end of the spectrum, you have well-behaved applications. For example, this could be 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. Such predictable workloads don't typically benefit from cloud characteristics.

In the middle of the spectrum, shades of gray exist. For example, you may have a classic overprovisioned workload. Such a workload example would be one that has a peak and you must overprovision for it. Assess the merits of moving such a workload to the cloud.

**Aligning With Other Strategies and Supporting Elements**

Cloud computing doesn't exist in a vacuum and neither should your cloud strategy. Ensure your cloud strategy aligns with existing strategies (such as those for security, the data center, and development and architecture). It mustn't reinvent or contradict them. Communication and negotiation are vital for success.

**Security**

Approach security and all the other supporting elements (such as technical architecture, infrastructure, staffing and procurement) by ensuring they align. Figure 6 describes these. If you include something
about security in your cloud strategy, ensure it also goes in your security strategy and vice versa, and that they align. Sometimes that may mean modifying the overall security strategy.

Figure 6. Cloud Strategy Document — Alignment and Exit Strategy

Cloud Strategy Document — Alignment and Exit Strategy

<table>
<thead>
<tr>
<th>Security:</th>
<th>Exit Strategy:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• State security principles</td>
<td>• Contracts with T&amp;C, SLA</td>
</tr>
<tr>
<td>• Identify responsibilities</td>
<td>• Data ownership, backup, getting data back</td>
</tr>
<tr>
<td>• Includes governance, compliance</td>
<td>• Lock-in, etc.</td>
</tr>
</tbody>
</table>

Action: Apply result to security strategy and cloud strategy

<table>
<thead>
<tr>
<th>Other Strategies and Supporting Elements:</th>
<th>By type of service</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Architecture</td>
<td>Development/Architectural issues</td>
</tr>
<tr>
<td>• Staffing</td>
<td>Multicloud strategies</td>
</tr>
<tr>
<td>• Data center ...</td>
<td>Strategy, not detailed plan</td>
</tr>
</tbody>
</table>

Action: Alignment with other strategies

Security (including governance, compliance and privacy) warrants a section of its own because it’s so important. Attitudes toward security have changed significantly. Originally, many people considered the public cloud too unsecure. Now, some organizations trust public cloud providers too much (see Revisiting the Top 10 Cloud Myths for 2020).

In Clouds Are Secure — Are You Using Them Securely?, we stress the importance of understanding roles in security. The top-tier cloud providers do an excellent job of securing the services they provide. For example, Amazon Web Services (AWS) secures the services — primarily IaaS — including virtual machines, storage and networking — but doesn’t secure the applications or data that you host there. You must ensure that the data you put in IaaS is locked down appropriately. It’s not the provider’s fault if you
leave your data unprotected. Security is a shared responsibility, but identifying roles and responsibilities in detail is critical to using the cloud securely.

Approach security with high standards using concepts such as tiering providers. Top-tier providers are excellent at security. But anyone can claim to be a cloud provider and may have a far lower level of security capability than a top-tier provider. Also, ensure you identify responsibilities in cloud security.

You must adhere to your existing security strategy or change it to accommodate the realities of cloud computing.

**Supporting Elements — Organizational and Staffing Issues**

Just as you must align cloud security issues with your overall security strategy, so you must align cloud staffing issues with your overall staffing strategy. Cloud computing will change your staffing requirements, depending on what level of cloud service you adopt. You’ll need different mixes of skill sets. You’ll probably need fewer people who manage servers directly, but more people who do higher-level tasks such as integration, network engineering, business analysis, vendor management and security. Growth opportunities will exist for some, and it’s important to involve the right people. That’s why you must include HR in this effort.

You should also discuss the cloud strategy council and cloud center of excellence constructs from an organizational perspective.

**Exit Strategy**

Cloud repatriation (moving workloads back from a public cloud) is rare. But it’s vital to have an exit strategy that describes dependencies and choices, even though you may never use it. Awareness of possibilities and planning for them is an important part of strategic planning. Several regulators, mainly in the EU and focused on financial services, now mandate an exit strategy.

Those organizations that do look at exit strategies often focus on contracts — aspects such as terms and conditions, and service-level agreements. Although how to get out of a contract is important, it’s just the beginning when it comes to an exit strategy. You must also examine issues such as:

- Data ownership
- Backup
- Getting back your data
- Portability

Include in your exit strategy both technical 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.

Make lock-in one of the main issues you discuss as part of your exit strategy. You can have lock-in in many different places: at the data level, the application level, the architecture level or the skills level. This may be what makes you examine multicloud and cloud-native issues.

Many say they want to follow a multicloud approach but note in their cloud strategy documents that they also want to be cloud-native. Although these concepts aren’t necessarily completely at odds with each other, they can be if you take them to their logical extremes. If you want to follow a multicloud approach and not be dependent on a vendor, then you should be careful in utilization of the native capabilities of a vendor. There are trade-offs. No simple answer exists, but you should handle these issues in your cloud strategy.

Organizations usually start with a few projects with one cloud provider. After initial successes, they soon have many workloads with that one provider. They also have a correspondingly large expense, and they may begin to worry that they’re too dependent on one vendor. As a result, they often start a procurement-driven multicloud strategy to encourage competition. Next, they begin a management strategy to obtain a single pane of glass for monitoring. Eventually, some reach the architectural issues, focusing on the portability of applications and the role of technologies such as containers, PaaS and open source.

When you consider SaaS vendors, take into account that many vendors are becoming pure-play SaaS providers. Fewer traditional on-premises offerings are available.

Focus your exit strategy on answering “what” and “why” questions. Cover the answers to “how” questions in a more detailed exit plan. Your exit plan should be workload-specific and describe how you will get out of a particular cloud situation if it doesn’t work out as planned.

Cloud Strategy in Practice

In practice, your cloud strategy will work as shown in Figure 7. You have established your cloud council, produced your cloud strategy and established your principles. You have also at least started to produce an inventory.
Figure 7. Cloud Strategy in Practice

Cloud Strategy in Practice

You’ve accomplished:

- ✔ Cloud council established
- ✔ Strategy
- ✔ Established principles
- ✔ Inventory and other elements in process
- ✔ Take action

Scenarios:

1. Request comes in for enhancement to existing app:
   - Consult inventory and apply principles to decide action

2. Data center strategy determines to close data centers in 2 years:
   - Use inventory and principles to determine action
   - Build cloud migration plan

Source: Gartner

For example, if you have decided to follow a cloud-first principle, when a request comes in to enhance an existing application, you’ll consult the inventory and apply the principles to the request. It becomes more complicated if your data center strategy is to close the data centers in two years. In that case, you must also start to build a cloud migration plan in which you find homes for everything. Unless you have that kind of an edict, there’s little 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. Data center and I&O-centric issues often drive the extenuating circumstances. But other considerations — such as application modernization, mergers and acquisitions, new product development, business resilience and other strategies — may trigger mass migrations.

The process of applying principles to an inventory prompts you to decide what to do with a workload. Figure 8 shows the different decisions you can make about a workload. We call these the “Rs.”
On to the Implementation/Adoption/Migration Phase

A cloud strategy is a living document. As such, it feeds the next phase of implementation (also called adoption or migration). Even if you’ve already started implementation, you can work on strategy and implementation simultaneously.

We’ve published several research notes to help you with the implementation phase, including:

- How to Begin Using Public Cloud Infrastructure as a Service
- 2021 Planning Guide for Cloud and Edge Computing
- Designing a Cloud Workload Placement Policy Document
- Innovation Insight for the Cloud Center of Excellence

Document Revision History

The Cloud Strategy Cookbook, 2019 - 2 April 2019
Recommended by the Author

A CIO's Guide to Strategy Development
Align Your Cloud Strategy With the Organizational Strategic Plans
Top 10 Tips for Avoiding the Most Common Mistakes in Cloud Strategies
Revisiting the Top 10 Cloud Myths for 2020
Hype Cycle for Cloud Computing, 2020
Innovation Insight for Multicloud Computing
NIST and Gartner Cloud Approaches Are More Similar Than Different