White Paper: **February 2023**

Benchmark Your Cloud Maturity: A Framework for Best Practices

Table of contents

Executive summary

The era of multi-cloud is here to stay. Once up and running in the cloud, enterprises typically face a set of common challenges: loss of control, staying ahead of security risks, and climbing cloud bills. With hundreds of users across multiple clouds consuming thousands of different services every day, cloud operations can become more complex than traditional tools or processes can handle.

Over the past decade, we have worked with thousands of organizations at all different stages in their cloud journey. During this time, we've identified patterns in the way that successful cloud management strategies mature as cloud usage grows and new challenges emerge. To help others on their cloud journey, we've established a framework that you can use to assess and improve cloud maturity across the three most critical areas of excellence:

- Financial management
- Operations
- Security and compliance

Three key areas of excellence

When it comes to driving success in the public cloud, many organizations find that the biggest hurdle they must overcome isn't related to technology. Some of the most significant challenges organizations face are getting their people and processes to adapt to a faster-paced, cloud-centric world. To help close this gap, leading organizations are establishing a formalized cloud center of excellence (CCoE), sometimes known as a cloud business office, cloud strategy office, or cloud program office. The CCoE is a cross-functional working group that governs the usage of the cloud across an organization and drives best practices across functions.

One of the early proponents of the term cloud center of excellence was Stephen Orban, who blogged about it in 2016. At the time, Orban was the global head of enterprise strategy at AWS (he has since become the company's general manager of AWS Data Exchange), and his vision for a CCoE involved a team responsible for developing a framework for cloud operations, governing the IT infrastructure and building out best practices throughout the business. More than four years later, this vision is becoming a reality at many enterprises. Typically, a CCoE will span three core areas of excellence: cloud financial management, cloud operations, and cloud security and compliance.

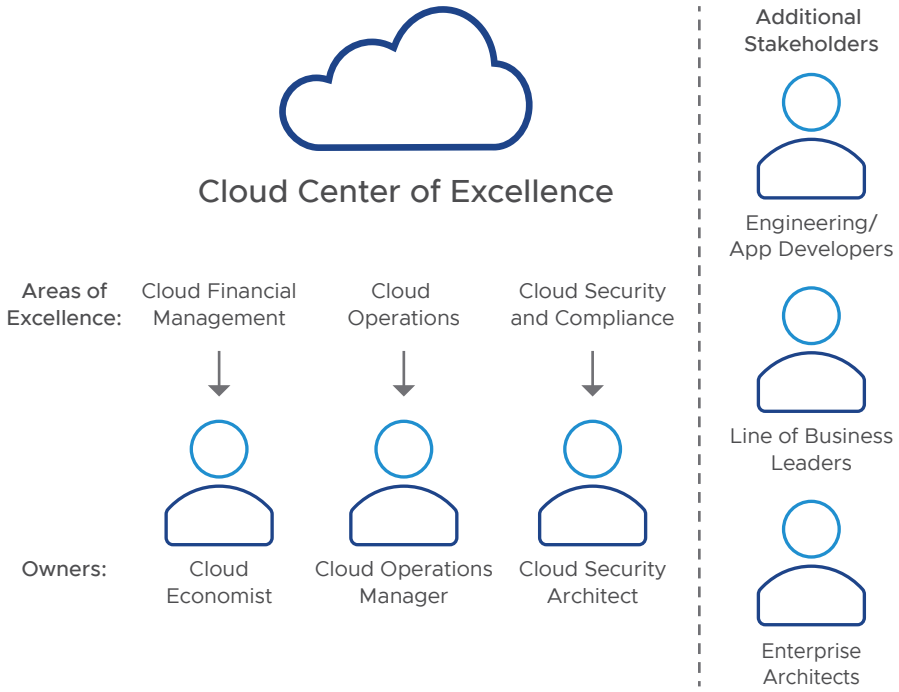

Figure 1: Example of a cloud center of excellence.

Cloud financial management

This is the process of continuously optimizing and aligning cloud investments with strategic business initiatives.

A mature cloud financial management function must:

- Profoundly understand how all components of a modern cloud environment contribute to total cost of ownership (TCO)
- Make business decisions based on accurate ROI analysis
- Cultivate financial accountability and ownership across groups

Cloud operations

This is the process of managing and delivering cloud services that meet the availability, performance, recoverability, quality and scalability needs of the business.

A mature cloud operations function must:

- Ensure operations meet and exceed business requirements
- Identify and act on areas to improve operational efficiency
- Drive operational consistency across groups

Cloud security and compliance

This is the process of proactively detecting and remediating vulnerabilities in your cloud environment.

A mature cloud security and compliance function must:

- Ensure continuous compliance with relevant standards
- Stay up to date with the changing threat and compliance landscape
- Translate business requirements into cloud security standards

Critical components to assess in a maturity framework

Once established, the owners of these areas of excellence must drive consistency across the organization and find opportunities to share best practices across teams and lines of business. An effective way to do this is to adopt a framework that can be used to drive improvement in key areas. The following is a framework you can use to compare progress against your peers and benchmark across business units and teams.

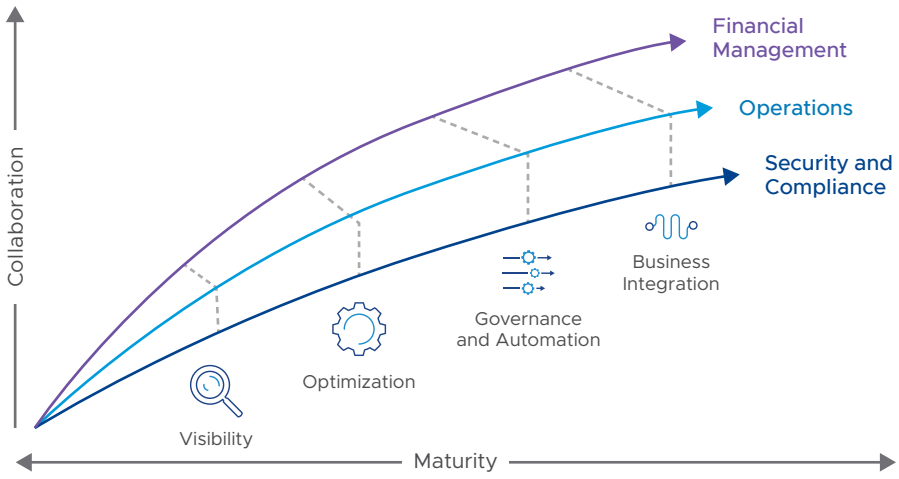

Figure 2: The cloud management maturity framework.

The four phases of multi-cloud maturity

From our work with thousands of organizations around the world at all different stages in their cloud journey, we've identified patterns and best practices for mature cloud management practices. These tactics often begin as an attempt to tame complexity as cloud usage scales, but ultimately transform into strategies that can fuel innovation and enable competitive differentiation. Each of the areas of excellence—financial management, operations, and security and compliance—will move independently through these four phases of maturity:

1. **Visibility –** A typical cloud journey begins with trying to address challenges around gaining visibility into a decentralized multi-cloud environment. Without visibility across all clouds broken down by business group, companies struggle to predict and forecast cost, identify security vulnerabilities quickly, and maintain consistent infrastructure. Cost is often the first area that an organization will tackle with regard to visibility, but usage, configuration, performance and security are all equally, if not more, important.
2. **Optimization –** The next step is optimization, which is the process of finding opportunities to be more efficient, whether it's in cost savings, time savings due to operational improvements, or tightening security parameters. At this phase, optimization processes may be manual, but a common best practice is to document the approaches they find beneficial for use across teams.
3. **Governance and automation –** Governance consists of defining the ideal state so you can monitor when drift occurs. Some companies equate this to setting up guardrails for their environment. Typically, the ideal state is an optimized state, whether it's cost, security or usage optimization related. Once governance policies are established, the next phase is to automate response and remediation of these policies, freeing up employee time for more critical tasks. Many organizations find that as their cloud grows, staff can't keep up with the sheer volume of information and the complexity of running production workloads across multiple clouds.
4. **Business integration –** This phase is about understanding exactly how your cloud strategy drives business transformation and impacts your most pressing corporate goals. For example, cloud key performance indicators (KPIs) are directly linked to cost of goods sold (COGS) and margins (cloud financial management), new product innovation/competitive win rate (cloud operations), and compliance with industry standards (security and compliance).

Optimizations are made continuously and automatically to align with the key drivers of your business, such as your go-to-market strategy. In this example, if your cloud financial management is fully integrated into your business, you're continually optimizing cloud costs to inform your pricing and packaging strategy. You've rightsized your operations to ensure you have the capacity to continually innovate and stay ahead of the competition without costly waste. And you're proactively addressing security and compliance issues so that you can win business in regulated sectors.

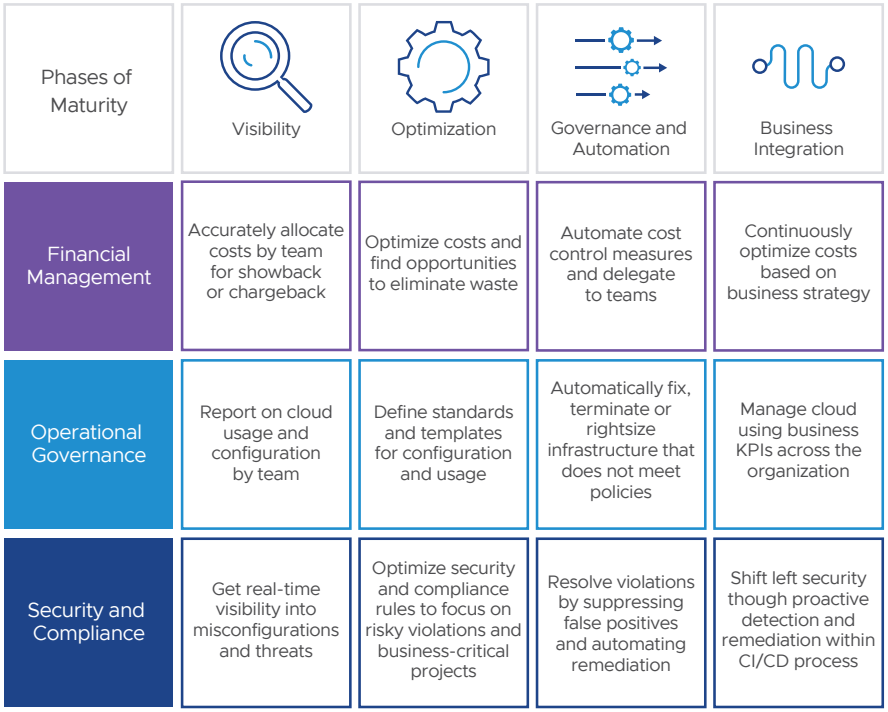

Figure 3: Deep dive into the phases of the maturity framework.

At any point in time, an organization will likely straddle different areas of maturity in the various areas of excellence. For example, they might have progressed to the governance and automation phase when it comes to operations but are still in the optimization phase for financial management and the visibility phase for security and compliance. Each of these areas of excellence does not operate in a vacuum; a strong thread of collaboration needs to run across the functions to ensure they can share and reuse organizational best practices. The biggest challenges when moving up the maturity curve are often related to people and processes rather than technology. Documenting and sharing best practices and successes from one function can provide a significant advantage for another.

Best practices for each stage of cloud maturity

While not all of these practices will work for everyone, after speaking with dozens of organizations, we've distilled several of the common best practices that enterprises adopt at each phase of maturity across the different areas of excellence. Every organization is unique in how quickly they will move through these phases, and progress won't always be linear or uniform—one area of the business unit or department may end up much further along in their journey than another. This is where the CCoE should act as a centralized service bureau to the business units, providing guidance, brokering connections, and consolidating and sharing the best practices for all to consume.

KPIs for success

- Cost of all untagged resources ($)
- Percent of environment with proper tagging in place (%)
- Percent of total bill charged back (%)
- Variance of budget compared to actual by application or team (%)
- Forecast accuracy (%)
- Security incidents per month by team (n)
- Security vulnerabilities identified per month per team (n)
- Mean time from vulnerability announced to all systems patched (n)

Best practices for visibility

Gaining visibility across cost, usage, security, performance, availability and configuration in a multi-cloud environment may sound like a simple task, but when your environment is spread across many accounts, clouds, regions and teams, it's often more difficult than expected. To truly master this stage, it's critical to not only gain visibility across all of these areas, but to report on them and how they align to the business unit, team, department, application or project that they belong to.

Having this business context is critical to understanding both the impact and the potential remediation of an identified trend before taking action. For example, if you discover an asset that is open and accessible to the internet, but you don't know if it's supporting a marketing application on the web or if it's an internal system with sensitive data, you won't know how to respond and remediate this potential threat.

In addition to visibility aligned to your business, it's also critical to have visibility aligned to personas. In a multi-cloud environment, there is a broader and more diverse set of roles that touch the cloud on a daily basis than ever before. Infrastructure and operations, engineering, DevOps, finance, security, application owners, and line of business stakeholders each have unique requirements for the data they need to see to make decisions. To be successful, these teams must be working with a common data set, so they can easily collaborate and troubleshoot when issues arise.

A typical cloud journey begins with trying to address challenges around gaining visibility and controlling costs. Without visibility across all of your clouds, broken down by business groups, applications or users, it's almost impossible to take the next steps to improve overall governance. Visibility spans cost, usage, performance, configuration, security and availability.

Best practices for optimization

Optimization is the process of finding opportunities to be more efficient and reduce spend or save time, without sacrificing functionality or required resources needed to meet your broader business objectives. At this phase, optimization processes may be manual, but organizations should start documenting approaches they find beneficial for use across teams.

While cloud gives the flexibility to scale up/down and pay for what you consume, you might overspend/overprovision without the right toolset. The inverse is also problematic: Not investing enough in cloud infrastructure could result in underperforming applications and a poor user experience.

Mature organizations have robust cloud cost optimization practices and teams that evaluate the best approaches to activities, such as rightsizing, elimination of zombie infrastructure, management of reservations, Committed Use Discounts or Savings Plans, lights-on/lights-off policies, and low-cost, short-lived compute options, such as Spot instances/virtual machines (VMs) or Preemptible VMs.

KPIs for success

- Percentage of infrastructure running on demand (compared to covered by Reservation, Savings Plan, Committed Use Discount, etc.) (%)
- Rightsizing savings (%)
- Effective cost per resource (i.e., $/compute hour) ($)
- Production incidents by application/team (#)
- Reverted deploys (%)
- Mean time to repair, mean time between failures (time)
- Number of security lapses (open ports, identity and access management failures, etc.) (n)
- Number of assets that do not meet configuration standards (wrong VM type, location, image, OS, tagging) (n)

Optimization isn't just about cost, however. Operational optimization involves finding opportunities to be faster and more efficient at day-to-day tasks and ensuring that infrastructure has a consistent and standard set of configurations. Security optimization is the process of proactively monitoring and suggesting remediation of security and compliance risks. For both of these areas, optimization is very closely tied to the next phase of governance and automation.

The key to success in this phase is to motivate and incentivize teams to take steps to optimize. In traditional engineering teams, there's little awareness of credence given to cost, configuration or security (although in the case of security, this is improving). For many organizations, the mantra is to enable developer productivity at any cost. While the first and foremost goal must be to enable developer speed and quality, there are ways to increase awareness and accountability related to cost, configuration and security without sacrificing productivity.

Some specific tactics include the following.

Visibility and alerts

Providing visibility, such as simply showing a leaderboard of the most optimized teams in rank order can drive positive results. Taking this a step further, another effective tactic for changing behavior is to show teams when there is an opportunity to optimize and what the outcome would be. For example, showing an engineer that if they were to pick a small VM or instance, they could save the company 50 percent in cost and they would still have more than enough performance to run their workload can help adjust behavior. It's important to integrate these alerts and reports into the familiar tools that are already in use, such as Slack or Jira.

Chargeback/showback

Similarly, in the realm of cost, many organizations successfully implement showback and chargeback strategies to help incentivize teams. Many companies find that when teams have direct financial responsibility for their actions, behavior changes rapidly. Organizations can start with a showback approach (which involves sending an invoice to teams and departments showing their spend, but not actually doing cross-departmental charges) before eventually implementing true chargeback.

Gamification

Many organizations have seen success by gamifying optimization. For example, you might set up a contest where the teams that take the most optimization steps for cost, security and operations can win a prize. At a large telecommunications company, the manager of cloud cost governance helped develop a game that rewards employees who identify opportunities to reduce or avoid cost, introduce process improvements, or automate optimization tasks. Some companies also call out low-performing teams, although depending on your company culture, this may or may not be an effective or appropriate technique.

Optimization is not a one-and-done activity. Optimization must be a continuous process to be truly effective. Of course, this can become extremely time consuming, which is what drives many organizations to the next phase of governance and automation.

Best practices for governance and automation

Governance is the process of defining best practices, and then getting notified (or taking action) when infrastructure is out of compliance or has drifted. Governance policies can be implemented in a few different ways, each with a set of advantages: in-band and out-of-band.

In-band

An in-band policy is evaluated before a user takes an action that would potentially violate best practices. The advantage of this approach is that it prevents users from taking actions that could be dangerous or expensive. The disadvantage is that it can potentially hamper user productivity and cause them to go around corporate IT.

Out-of-band

An out-of-band policy is evaluated after a best practice violation is detected. The advantage of this approach is that it stays out of the users' way and performs cleanup after the fact. Conversely, the disadvantage is that it allows users to violate best practices and can be damaging if they aren't fixed in a timely manner.

In addition to in-band and out-of-band detection, there are two primary ways companies take action on governance policies: guidelines and guardrails.

Guidelines

Guideline policies will communicate a risk boundary via an alert that informs the user of the best practice, but will not take action to prevent or correct the action.

Guardrails

Guardrail policies will both communicate and take action to correct a violated best practice.

Table 1 shows an example of what happens in each scenario when a user violates, or attempts to violate, a best practice.

	In-Band	Out-of-Band
Guideline	Before deploying, user is notified that they are violating a best practice, with instructions on how to properly deploy the resource. User can ignore the notification and process with deployment.	After deploying, user is notified that their recent deployment violated a best practice. Notification includes instructions on how to fix their mistake and conform to the best practice.
Guardrail	Before deploying, user is notified that they will not be able to deploy until they fix the violation, or the violation is automatically corrected before deployment.	After deploying, user is notified that their recent deployment violated a best practice and that it has been automatically fixed.

Table 1: Defining in-band and out-of-band governance.

For many organizations, the governance and automation phase progresses iteratively, with first defining the best practices, then implementing guideline policies, then slowly adding guardrail automation to as much of their environment as possible to free up employee time for more strategic tasks.

The first step of defining the best practice state, or the rules of the road, will be different for every organization, but there are some common approaches that can serve as a starting place for most organizations.

Financial management governance

The path for financial management governance is well trodden. Many organizations start with setting budgets and then tracking adherence to them. They'll also define what's in the realm of normal or acceptable for a cost increase so they can quickly find anomalies. On the optimization front, they'll identify the appropriate range for percent of infrastructure running on demand compared to lower-cost alternatives.

Operational governance

There are several operational governance standards that can help form the basis of an organization's operational governance policy, the most common being the AWS Well-Architected Framework. Organizations have fully embraced the Well-Architected Framework and report that it translated well into business terms, helping teams understand why good engineering matters and turns into business value. While the Well-Architected Framework is obviously cloud-specific, it contains concepts that are easily extendible to other clouds. A framework such as this one will only take you so far, as you'll also need to define what your organization considers to be standard configurations and infrastructure. Areas to consider include tagging policy, standards for configuration, region, infrastructure types, OS, as well as high/low watermarks for underutilized infrastructure.

Security and compliance governance

In the realm of security and compliance, there are many standards and governing bodies that provide robust sets of governance policies. Most organizations will start with an industry-specific standard and the Center for Internet Security's standards for individual clouds, and customize them to meet their specific needs.

Once these governance rules are defined, the next step is to automatically alert on and remediate as many as possible. Because this phase requires the greatest shift in mindset and changes to existing processes, this step is the most challenging and time consuming for many organizations.

Companies that have already crossed this chasm offer the following advice.

Frame governance as helpful rather than a hindrance. When many people hear the term "governance," they immediately think of rules and policing, but it's possible to turn these conceptions around with framing.

Start with simple automation and ramp up slowly over time. Taking the initial steps from governance guidelines to governance guardrails can be a daunting one. Experts advise to start slow and ramp up over time. Begin with an approval workflow so a human is giving the final OK before action is taken.

KPIs for success

- Percent of policies in compliant state (n)
- Cost optimized over time ($)
- Cost optimized per policy over time ($)
- Time saved as a result of policies (hours)
- Number of reservations automated (n)
- Time to remediate security violation (hours)
- Service availability (%)
- Time to deploy (hours)

You can then progress to low-stakes automation, such as terminating unattached storage after a certain amount of time or old snapshots. Eventually, you can progress to more advanced automation, such as lights-on/lights-off policies, shutting down non-production infrastructure with improper tagging, and security violation remediation.

Opt out of instead of opt in to governance policies. To kick-start adoption of automated governance policies, Cathal Cleary, director of cloud services for VMware Engineering Services, set up policies to be opt out instead of opt in. This means that policies will apply universally to all assets unless they are tagged specifically to be skipped. For example, a policy might automatically delete all snapshots once they are 90 days old unless they have the tag value nodelete.

Ensure you can scope automation by environment and flag exceptions. Automation works best as a finely tuned instrument rather than a brute-force object. For every governance policy, there will be exceptions, and for every line of business, there may be different policies. For example, there are valid reasons to have object storage that is open and accessible to the public, but a brute-force automated policy will continuously try to flag and shut it down. Using tags and other attributes to scope your automation will help alleviate some of this burden.

Best practices for business integration

At this phase, you already have complete visibility into all of your cloud environments, continuous optimization and well-defined governance policies that are automated as much as possible. The last step is to integrate your cloud processes into business processes and ensure that KPIs are aligned so everyone is working toward a common goal.

This concept may seem a bit broad and abstract, so let's look at a few concrete ways organizations are making business integration a reality.

Integrate with business systems

One small step that has an outsized impact is integrating metrics from the CCoE into business systems, and vice versa. For example, some organizations integrate their cloud management platform into their budgeting and accounting software so entries for financial chargebacks and accruals can flow automatically. In the security world, this might entail integrating cloud security and compliance alerts and reports into a governance, risk and compliance (GRC) solution. An even simpler integration into a business system that will have a positive impact is integrating cloud management solutions into communication tools such as Slack, Jira and Confluence. This is key for embedding cloud management processes into the day to day of users both inside and outside of IT.

KPIs for success

- Cost per customer ($)
- Cloud spend as a percentage of revenue (%)
- Reduction in COGS over time (%)
- Cost of revenue over time ($)
- Time to bring new services to market (time)
- Compliance issues open (n)
- Mean time to detect (time)
- Customer satisfaction (typically using Net Promoter Score)

What does contributing to business initiatives look like in practice?

Segment, a fast-growing B2B SaaS company, was challenged by their board of directors to improve gross margins. Tido Carriero, chief product development officer at Segment, took this challenge to his team, asking them to find ways to reduce their COGS. Over the course of a year, the team investigated all the top drivers of cost for each product and took actions, such as rightsizing, rewriting inefficient code, and adding availability zone awareness into applications. Ultimately, they were able to help increase gross margins by 20 percent within a year. These activities also led Segment to revisit packaging and pricing for their product lines to better align pricing to COGS.

Contribute to business initiatives

Understanding and contributing to top-line business initiatives is a successful strategy for organizations at this phase. This will help raise the profile and awareness of the CCoE, which can lead to improvements in adoption and funding. This could be an initiative to reduce the bottom line or to produce high-quality products faster. Another example is within the realm of compliance; if there's a business initiative to achieve or maintain a certain compliance standard, the cloud security and compliance function can make significant contributions.

Align to business metrics

Framing cloud management metrics in the context of the business has the dual benefit of providing business context to IT and engineering teams, and allowing business users to more easily understand the impact of the CCoE. This might be reporting on cloud costs as how they contribute to COGS, or as cost per customer to support. The team at Segment (see sidebar for details) found it useful to report out on cost per million API calls because API calls were a central cost driver in their application. This was a helpful, normalizing metric for them because it should stay constant even as they scale.

Business integration isn't just about numbers and systems, however. It's also about people across different functions collaborating to achieve a common set of goals. The more embedded your CCoE is into the business, the more effective it will be. The more a CCoE feels like the hub of a community, rather than a governing body, the more effective it will be.

Five key takeaways

Whether you're just getting started on your journey to a more mature cloud management practice or are already further down the path, here are five key takeaways that can help you get to the next level:

1. Start with a formal or informal cloud center of excellence. The first step to improving cloud maturity requires the formation of a team to help drive the organizations forward. This team may be an informal group of individuals with a common goal in improving cloud maturity or a more formal committee of stakeholders. The key is that they can work together to drive improved processes cross-functionally.
2. Keep your eyes on the prize. Stay focused on your organizational goals, and ensure that cloud management practices align with these objectives. For example, if you initially adopted the cloud to improve agility, flexibility and innovation, be wary of any cloud management practices that might get in the way of developer productivity or slow down velocity.
3. Benchmark against peers. One of the benefits of using an established maturity framework is that you can use it to compare your progress to other organizations in your sector. Join industry communities and discussion groups to compare notes and learn best practices from others on the same journey.

4. Establish KPIs early and measure results consistently. Throughout this white paper, we suggest different KPIs you can adopt to track success as you move through the various phases of maturity. Keeping track of progress over time, and benchmarking against yourself, can help show which actions are having the greatest impact.
5. Don't be afraid to break down silos. Successful business and IT transformation is predicated upon the ability for teams across many different functions to communicate and work together effectively. This might mean bringing together teams that have never worked together, such as finance and IT, or potentially disparate business units. Give the teams time to understand each other's objectives and backgrounds before rushing ahead with joint projects. The more the groups understand each other's motivations, the less friction the project will experience.

Learn more about how VMware Tanzu CloudHealth® can help your organization progress on your cloud maturity journey.

Item No: 1703106aq-wp-bcm-your-cld-mat-a4 2/23