White Paper: **September 2023**

Global Assessment of Cloud Management Maturity

Table of contents

Executive summary

Over the past decade, we have worked with thousands of organizations at all different stages in their cloud journey. From our work, we've identified patterns and best practices for building a cloud center of excellence (CCoE) with mature cloud management practices.

To help others on their cloud journey, we've established a cloud management maturity model. This framework helps the broader cloud community assess their cloud maturity and identify areas for improvement across the three most critical areas of excellence:

- Cloud financial management
- Cloud operations
- Cloud security and compliance

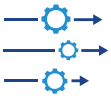
Typically, organizations that invest in the public cloud move independently within each area of excellence through four phases of maturity.

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 groups, companies struggle to predict and forecast costs, identify security vulnerabilities quickly, and maintain consistent infrastructure.

Optimization

This process finds opportunities to be more efficient, whether it's in cost savings, time savings due to operational improvements, or tightening security parameters.



Governance and automation

Governance consists of defining the ideal state of your environment so you can monitor when drift occurs. 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.

Business integration

This phase is about understanding exactly how your cloud strategy drives business transformation and impacts your most pressing corporate goals.

In July 2020, we launched the Cloud Management Maturity Assessment, an online tool designed to help the cloud community measure their organization's cloud management strategy against our framework, identify which phase of cloud management maturity aligns with their current practices, and recommend best practices to advance to the next phase in each area of excellence.

The assessment is based on a brief survey in which respondents can select and measure against one or more of the key areas of excellence (cloud financial management, operations, and cloud security and compliance). Completing the assessment also generates a report that shows how a respondent's results compared to those of other respondents in the same industry. The report also provides recommendations for the respondent to progress in their cloud journey based on their current stage of maturity.

This white paper analyzes the survey results of more than 950 respondents worldwide from December 2021 through December 2022. Additional information on the methodology of our analysis can be found in the appendix.

Key findings:

- The majority of respondents are in the IT industry, in IT operations roles, and are based in the Americas.
- 49 percent of respondents have a multi-cloud strategy, and 14.3 percent of respondents use a combination of Amazon Web Services (AWS) and Microsoft Azure.
- Across all three areas of excellence, the majority of respondents are still in the visibility phase of maturity.
- Respondents appear to be more mature in cloud financial management than the other areas of excellence.
- More than 50 percent of respondents under cloud operations indicated that they either don't have a tagging strategy at all or that they have one defined, but it is not strictly followed.
- The majority of respondents to the security and compliance questions do not have real-time insight into security events, changes and risks; the ability to visualize resource configurations and relationships between resources; or an understanding of security trends, including history and progress in reducing risks.

About the Cloud Management Maturity Assessment

The Cloud Management Maturity Assessment was created to compare your progress against your peers and benchmark your maturity across business units and teams. As a disclaimer, when we talk about maturity, we aren't talking about the competence of your organization in the cloud. Instead, we mean the maturity of your organization's ability to scale operations and security in the cloud.

Within the assessment, respondents are asked demographic questions (e.g., industry), cloud strategy questions (e.g., cloud providers being used), and diagnostic questions for each area of excellence (financial management, operations, and security and compliance) that correspond to the four phases of maturity (visibility, optimization, governance and automation, and business integration).

At any point in time, your organization will likely straddle different phases of maturity in the various areas of excellence. Each of these areas of excellence do 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. Documenting and sharing best practices and successes from one function can provide a significant advantage for another.

For the scoring methodology, see the appendix.

Demographics

As part of this white paper, we analyzed the submissions from a sample size of 790 respondents. For this analysis, the data was scrubbed to remove respondents who, for example, indicated "Test" as the company name.

Industry

Out of approximately 19 different industries, the top five industries based on the percentage of respondents included IT, financial services and insurance, education, digital marketing and advertising, and healthcare and life sciences. The majority of respondents (approximately 35 percent) work in the IT sector.

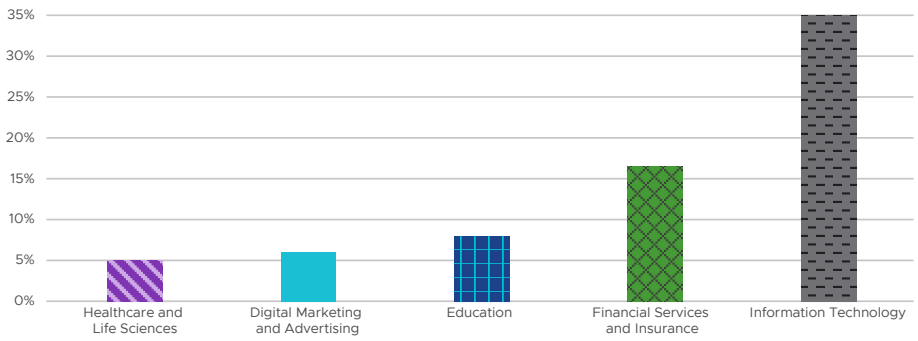


Figure 1: Top five industries by percent of respondents.

Job title

Out of 17 job title options across financial, operational and security roles, the majority of respondents indicated that they work in IT/infrastructure and operations. The top five job titles by the percentage of respondents were other, IT admin, architect, cloud ops and CIO. Due to the nuances of job titles across various industries and companies, it's no surprise that "other" was the most popular option at 16.9 percent. Due to the setup of the assessment, respondents who selected "other" were not given the option to write in their own job title, therefore we don't have additional details as to what represents that group.

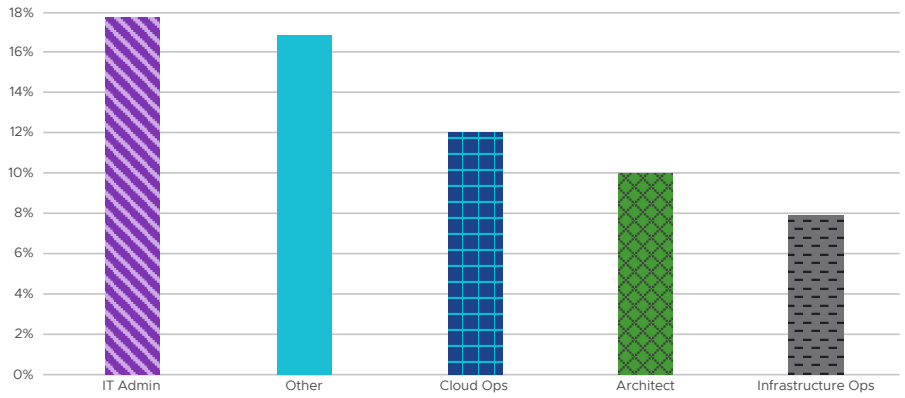


Figure 2: Top five job titles by percentage of respondents.

Geography

Although only available in English, the assessment is accessible for respondents via the VMware Tanzu CloudHealth website. Based on the responses, we did have representation across various countries, resulting in a geographic breakdown of 46 percent of respondents in the Americas (AMER), 31 percent in Asia-Pacific (APAC), and 23 percent in Europe, the Middle East, and Africa (EMEA).

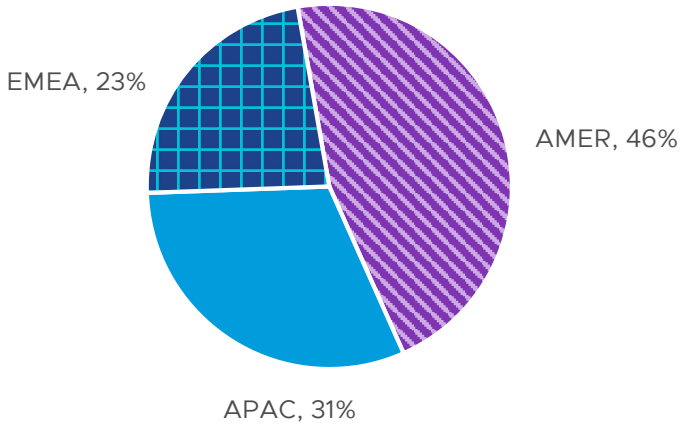


Figure 3: Percentage of respondents by geography.

Key findings: cloud strategy and usage

When it comes to driving success in a multi-cloud environment, many organizations find 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 CCoE, a cross-functional working group that governs the usage of the cloud across an organization and drives best practices across functions.

In this section, we explore survey responses that provide insight into the decisions that businesses are making in the cloud, including the clouds they are using, key initiatives and barriers. For more mature organizations, these discussions and decisions are typically led by the CCoE.

What best describes your company's cloud strategy?

The first question was intended to gauge the cloud strategy among the organizations that responded. 49 percent indicated they have a multi-cloud strategy. This aligns with separate data that currently shows that 52 percent of our customers use Tanzu CloudHealth to manage two or more public/hybrid clouds.

The assessment results also capture that 20.7 percent of organizations are on-premises and looking to migrate, and 21.5 percent are using a single public or private cloud. For the respondents who indicated that they don't have or are unsure of their company's cloud strategy, a CCoE can be a critical first step to understand how their teams are using public cloud services.

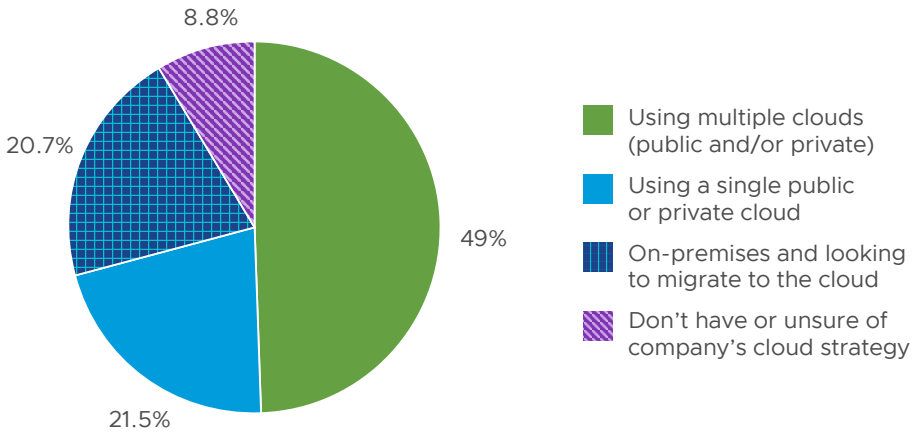


Figure 4: The cloud strategy being employed by percentage of respondents.

What cloud service providers are you currently using?

Respondents were asked to select the cloud service providers they are currently using. The possible options were AWS, Azure, Google Cloud Platform (GCP), VMware Cloud™ or VMware vSphere®, or Oracle Cloud Infrastructure (OCI). Based on the submissions, there were approximately 30 different combinations of clouds, with the top five being:

1. AWS – 25.6 percent
2. Azure – 20.3 percent
3. AWS and Azure – 14.3 percent
4. AWS, Azure and GCP – 7.2 percent
5. AWS, Azure and OCI – 3.1 percent

These results were fairly consistent with the position of the leading public cloud providers in the market, with AWS being the most selected option, followed by Azure. Due to the number of respondents who indicated they have a multi-cloud strategy, there were several multi-cloud combinations that made the top five. It is worth noting that the percentage of respondents who indicated they are using a single public cloud does not exactly match the percentage who selected a specific single cloud provider. This can be the result of respondents who might not have seen other clouds listed among the options, which can account for the difference.

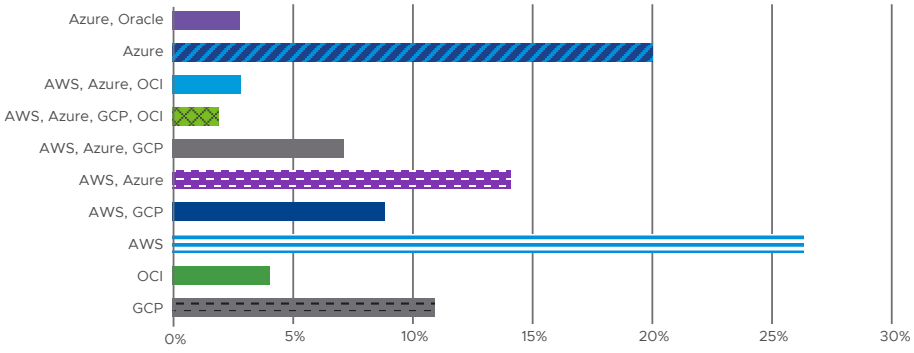


Figure 5: Top 10 cloud combinations.

What are your top three cloud initiatives for this year?

Respondents were asked to select their top three cloud initiatives for this year out of nine potential options:

- Better financial reporting on cloud costs
- Move from on-premises to cloud
- Expand use of containers
- Implement governance policies and automate actions
- Optimize existing use of cloud (cost savings)
- Implement continuous integration/continuous delivery (CI/CD) in the cloud
- Migrate additional workloads to the cloud
- Govern business unit IT
- Not sure/other

Of the 950 respondents, more than 53 percent selected these as their top three:

- Better financial reporting on cloud costs
- Expand use of containers
- Optimize existing use of cloud (cost savings)

Many businesses and supply chains were impacted significantly as the world shifted to combat the COVID-19 pandemic. The results of this question are consistent with what we've seen in the market and heard from our customers. Regardless of whether an organization is reducing, shifting or even increasing their cloud spend, the pandemic and the ensuing economic disruption intensified focus on accountability for what their teams are spending. This correlates with separate Tanzu CloudHealth data that showed a 186 percent increase in purchases via cloud service providers' committed use discount pricing options, such as Reserved Instances or AWS Savings Plans, among enterprises from April 2020 to May 2020, as the long-term nature of the pandemic settled in. Many organizations are scrutinizing their spending and focusing on optimization across their business, and operational expenses related to cloud usage were clearly an extension of that.

Containerization also factors in, as businesses seek to increase developer productivity and improve resource efficiency. In a recent survey of members of the Tanzu CloudHealth Customer Advisory Board, the majority of respondents indicated that 0–24 percent of their environment is containerized currently, but that they expect more than 25–75 percent of their environment to be containerized in the next 12 months.

What are the top three barriers to effective cloud management in your organization?

Respondents were asked to select their top three barriers out of eight potential options:

- Lack of cloud expertise
- Miscommunication across lines of business (LOBs)/departments
- Lack of a defined process and management support
- Trouble integrating with existing systems
- Complexity in migrating legacy applications
- Security and compliance concerns
- Complexity of reporting and managing cloud costs
- Not sure/other

Of the 950 respondents, more than 46 percent selected the following as their top three:

- Lack of cloud expertise
- Complexity of reporting and managing cloud costs
- Security and compliance concerns

Public cloud adoption has taken off over the past decade as organizations seek to leverage the agility and flexibility that the cloud offers, with many organizations still migrating. However, with new technology comes new challenges. A lack of cloud expertise, defined processes and management support are key challenges that we continue to see from the cloud community. Some organizations struggling with these challenges can benefit from building a CCoE to drive the success of their cloud strategy, while others might benefit from the guidance and expertise of a managed service provider.

Concerns around security and compliance are consistent with various other surveys and industry research that we've seen. It would be surprising to know of an organization that is not concerned about security threats and potential data breaches, especially in a time when businesses are forced to adapt to remote working models.

Areas of excellence

At the beginning of the assessment, respondents have the option to select one or more areas of excellence that they would like to assess. Of the 950 respondents, almost 50 percent participated in each category:

- 666 respondents assessed their cloud financial management
- 619 respondents assessed their cloud operations
- 450 respondents assessed their cloud security and compliance

The vast majority of respondents fell in the visibility phase of each area of excellence. Figure 6 shows the percentage of respondents that landed in each phase of maturity across the three areas. Note that the percentages are based on the number of respondents who participated in that category, with each column totaling 100 percent. For example, the 80.48 percent visibility in financial management is based on the 666 people who assessed their maturity in that area.

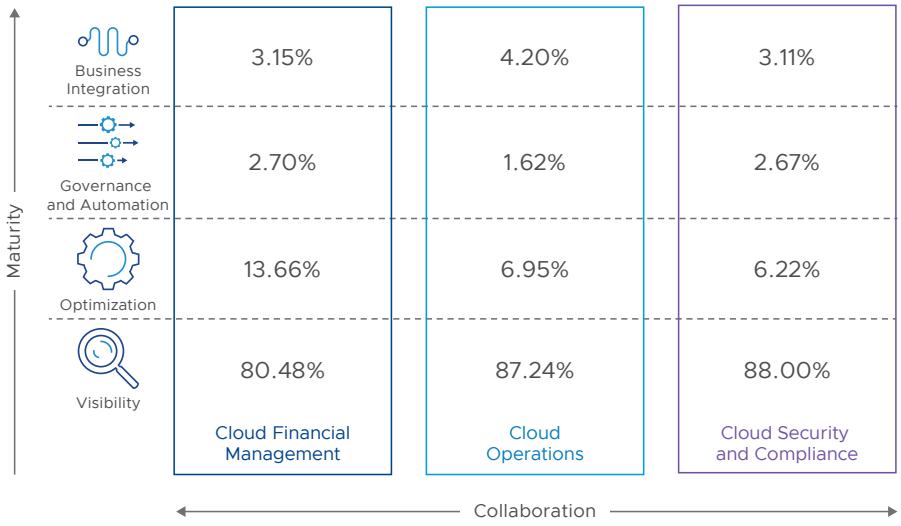


Figure 6: Percentage of respondents that landed in each phase of maturity across the areas of excellence.

Cloud financial management

Cloud financial management (CFM)—sometimes known as FinOps or cloud cost management—is a function that helps align and develop financial goals, drive a cost-conscious culture through best practices, establish guardrails to meet financial targets, and gain greater business efficiencies.

However, cloud financial management isn't a one-time exercise; it's a continuous process. A mature CFM function helps the business meet its goals and establish best practices within the CCoE. With the ever-changing nature of the cloud, the goal of CFM is to continuously optimize and align cloud investments to strategic business initiatives.

In this section, respondents were asked four questions:

- What cost accountability practices do you have in place?
- How do you eliminate waste and reduce costs?
- What automated cost controls do you have in place?
- How do you align cloud costs to your business?

The main reason the majority of respondents are in the visibility phase is that 60 percent indicated they have a basic understanding of costs/usage and are looking for detailed cost visibility. Considering that the first question encouraged respondents to select all that apply, ideally we would have liked to see closer to 80 percent of respondents having basic visibility into their costs and usage, noting that just more than 30 percent of respondents are still on-premises and migrating. 20–30 percent of respondents have visibility into cloud spend by business groups, perform showback or chargeback, have teams tracking monthly spend against their budget, and leverage executive-level cost reporting.

The optimization question provided options for rightsizing and discount management, in which 52 percent of respondents are manually identifying unused or underutilized resources, and 27 percent are using spreadsheets to calculate discounts and reservation purchases manually. For these respondents, manually using spreadsheets is a time-consuming and error-prone process. This indicates a business justification for use of a cloud management platform such as Tanzu CloudHealth.

For governance and automation, 46 percent of respondents do not have any automated cost controls in place. Examples include out-of-the-box alerts, cost spikes and budget alerts, or rightsizing policies. Very few respondents (less than 10 percent) have more advanced automated cost controls related to reservations and zombie infrastructure.

The last phase of maturity is business integration, in which the CCoE is aligned with executive management and the organization is integrating with business intelligence tools, gamifying cost optimization, and mapping cloud costs to business key performance indicators (KPIs), such as cost of goods sold. 43 percent of respondents indicated that business alignment is not in place, while 20 percent indicated their CCoE is aligned with their executive team.

Although the cloud financial management function is seeing some organizations progress into optimization and governance stages, there is still a lot of opportunity for improvement.

Cloud operations

Cloud operations 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, and drive operational consistency across groups.

The main reason the majority of respondents are in the visibility phase of cloud operations is that more than 50 percent indicated they either don't have a tagging strategy at all or they have one defined, but it's not strictly followed. This answer significantly impacts a respondent's ability to place at a higher phase of maturity because they lack a foundational element of cloud management.

Diving a bit deeper, in this section, respondents were asked five questions:

- How are you able to report on cloud configuration and usage?
- What are your existing cloud capabilities?
- What governance controls do you have in place?
- What level of automation do you have for managing your environment?
- How do business KPIs align to cloud operations and usage?

The first question pertains to the visibility phase of maturity, and only 21 percent of respondents indicated they have a well-defined strategy. Less than 12 percent are enforcing tagging. Although the majority of respondents cannot place into a higher level of maturity, they were still able to answer the remaining questions.

For the second question, we were looking to gauge what optimization capabilities and processes are in place, such as rightsizing, granular reporting by team, and having a resource-level inventory of all cloud services. 37 percent of respondents indicated they can show cloud usage in a simple graphical form from multiple sources, but only 25 percent or less indicated they have any of the aforementioned capabilities.

The third phase of maturity is governance and automation, and for the cloud operations function, we separated these into two questions. Generally, many of our customers are leveraging policies and alerts to drive consistent best practices across their organization. However, automation is still something that not everyone takes advantage of or feels comfortable doing. From the assessment results, we can see that 22 percent of respondents have no governance controls in place, but 32 percent do have standards (approved configurations) for their cloud infrastructure. Similarly, 29 percent also indicated they do not have automation in place. Overall, the majority of respondents are not taking advantage of actions with approval systems, fully automated actions, or auto-scaling capabilities.

Lastly, similar to the cloud financial management function, many respondents (31 percent) do not have business alignment in place. Only 18 percent have initiatives being driven top-down with cross-organizational KPIs. This represents a clear opportunity for these organizations to build a CCoE or to formalize the CCoE more broadly across their business.

Cloud security and compliance

Cloud security (or cloud infrastructure security) is a function that implements organizational policies and processes to protect data and infrastructure resources in public clouds. A mature cloud security and compliance function ensures your organization's cloud accounts and services are configured correctly to encrypt data, prevent unauthorized access to resources, and maintain regulatory compliance—all without slowing down innovation.

Security and compliance are regularly a top-cited concern for organizations, as confirmed by various analysts and market surveys. Despite this, the majority of respondents are in the visibility phase of their maturity.

Within this section, we asked four questions:

- What level of visibility does your cloud security team have?
- How do you prioritize cloud security and compliance risks in your organization?
- How do you scale the resolution of security violations across cloud environments?
- How do you integrate security and compliance across business functions?

The visibility question showed no clear majority response. Of respondents, 20–30 percent indicated they have centralized visibility into resources across cloud providers, monitor security and compliance based on best practices and industry standards, or have real-time insight into security events or risks. Similar to the cloud operations function, the lack of visibility into resources is why the majority of respondents were placed into the visibility phase.

For the second question, 35 percent of respondents indicated they prioritize security violations based on quantifiable risk. 25 percent or less also allow exceptions to security rules to reduce false positives for engineering teams, selectively enable or disable security controls based on environment and context, or build custom rules and frameworks.

Also similar to the other areas of excellence, the majority of respondents have implemented limited automation, if any. Of respondents, 33 percent claim engineering teams fix violations manually, and 20 percent said the security owner educates engineering teams on how to fix security violations. In other words, the security owner is instructing the team on how to remediate any violation, but this is a manual process. More mature organizations in this phase would use automation to bulk-remediate key existing violations while others are fixed manually, build guardrails to auto-remediate new violations through predefined actions, and enable engineering to review and fix violations through automated action.

For the business integration question, 20–28 percent of respondents indicated they have the following capabilities: stakeholders are informed (e.g., execs, LOB managers) about security and compliance posture through reports, engineering teams proactively detect and fix violations at the time of deployment (CI/CD), and the security operations center (SOC) and incident response integrate cloud inventory and risk insights into threat analysis. Based on the responses, it's clear these organizations need to improve visibility into security and compliance posture, and the use of a cloud management platform tailored to security and compliance would ease the burden on the engineering teams and security owners who are manually reporting, identifying, and remediating violations and misconfigurations.

Recommendations

As previously mentioned, success in the cloud hinges on the ability of organizations to collaborate cross-functionally to ensure alignment to business initiatives. We recommend that all organizations start with a formal or informal CCoE. When building a CCoE, it's imperative to have representation across key functional areas, as well as executive support and buy-in.

This section lists our recommendations across the four phases of cloud management maturity. In some cases, the recommendations might have already been implemented in your organization. The question then becomes: Are teams and business units operating independently of one another? Are all business units developing from a shared cloud strategy and documented best practices? If not, then these recommendations need to be discussed more broadly, and you need to check that you have the right stakeholders represented in your CCoE.

Get started

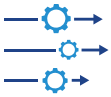
Take the Cloud Management Maturity Assessment.

Visibility

1. Develop a consistent tagging strategy to report on how infrastructure impacts business units, teams, departments, applications or projects, and to better identify and allocate spend and usage.
2. Define and document what your organization considers to be standard configurations and infrastructure. Areas to consider include tagging policy, region, infrastructure types, OS, as well as high/low watermarks for underutilized infrastructure.
3. Build reports and dashboards based on business groupings to improve collaboration and drive accountability. Collaborate on best practices, such as chargeback and showback across various teams, to standardize operating in the cloud.
4. Enable log collection and event alerting by default in each cloud account.
5. Restrict third-party access to critical applications through appropriate roles and maintain least-privilege access for all internal users and resources with identity and access management (IAM) roles.

Optimization

1. Motivate and incentivize teams to take steps to optimize. 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.
2. Eliminate infrastructure waste by terminating idle (zombie) infrastructure and rightsizing assets to improve utilization.
3. Leverage upfront commitments. All the major public cloud providers offer incentives for making an upfront commitment in exchange for a discount. These commitments are often called reservations or Savings Plans.
4. Target controls based on application or business requirements. To help maximize the impact, the controls must be paired with detection techniques focused on prioritizing issues with the highest security risk.
5. Narrow down your focus. Monitor security anomalies and guide vulnerability management efforts to harden parts of your cloud environment where you observe suspicious activities.



Governance and automation

1. Leverage third-party operational governance standards (e.g., AWS Well-Architected Framework) to help form the basis of your operational governance policy.
2. Define operational best practices, implement guideline policies, and then add guardrail automation to as much of your environment as possible to free up employee time for more strategic tasks.
3. Start with simple automation and ramp up slowly over time. Ensure you can scope automation by environment and flag exceptions.
4. Segment security actions into ones that can be fully automated and those that need human intervention.
5. Automate lights on/lights off tasks for non-production infrastructure on weekends or weeknights through scheduling. You can also automate entries for financial chargebacks and accruals through APIs and integrations.

Business integration

1. Establish KPIs early and measure results consistently. Keeping track of progress over time and benchmarking against yourself and peers can help show which actions are having the greatest impact.
2. Benchmark against your peers. Join industry communities and discussion groups to compare notes and learn best practices from others on the same journey.
3. Establish common goals by aligning cloud financial management metrics to business metrics, such as gross margins and cost of goods sold.
4. Integrate alerts and reports into tools that you already use across provisioning and orchestration, configuration management, and monitoring.
5. Adopt a continuous security model with the objective of building security checks right into the CI/CD pipeline.

Keep in mind that building a cloud center of excellence and implementing these recommendations and best practices are not done overnight. As the adage goes, “Rome wasn’t built in a day.” In a time when remote working is becoming the new norm, make sure you are frequently communicating across the organization and marching toward the same goals.

Appendix

Scoring methodology

Within the Cloud Management Maturity Assessment, the only sections that contribute to the score and placement along the framework are the sections for the three areas of excellence (cloud financial management, cloud operations, and cloud security and compliance). The demographic information gathered does not contribute to the placement. However, the industry information is used to provide respondents with benchmarks against their industry peers. The strategic questions also do not contribute to the scoring placement; they were included for informational purposes and to help us evaluate and confirm our assumptions about the market.

The questions within each area of excellence are intended to represent the various phases of the maturity model, with the first question pertaining to the visibility phase and the last question for the business integration phase. For each question, the available responses to select from are given a numerical score, and each question contains an entrance and exit score to proceed to the next question.

The first question is intended to capture the visibility phase. For this specific question, the entrance score is 0 and the exit score is 15. Depending on the question, the more options you select (given that you can select more than one response for each question), the higher your score will be, and you will move on to the next phase of maturity.

Within each question, the responses are weighted based on how advanced the action is. For example, selecting none would be a 0, whereas selecting an answer with automation can be scored at 25. Overall, if you select what is considered as the least advanced response, you will not score high enough to move on.

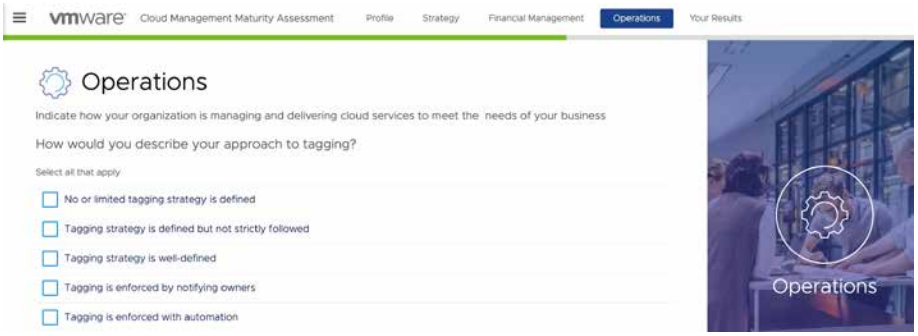


Figure 7: The first question in the cloud operations category.

As highlighted previously, the majority of the respondents indicated they either don't have a tagging strategy at all or have one defined, but it is not strictly followed. Not having a tagging strategy means the respondent was awarded 0 points. If they selected that the tagging strategy is defined but not strictly followed, they would receive 5 points, which is still not sufficient to score out of that category. This is why the majority of respondents were in the visibility phase of maturity. Had they, for example, selected "Tagging is enforced with automation," they would have received a score of 25 and advanced to the next phase of maturity.

Even if a respondent does not score out of the visibility phase, they will still be able to answer the remaining questions. However, those answers will not contribute to their score and placement.

Related resources

Continue your cloud management journey with us. Check out these additional white papers focused on cloud maturity and driving success in the cloud:

- Benchmark Your Cloud Maturity: A Framework for Best Practices
- The Next Generation of Cloud Management Starts with a Cloud Center of Excellence
- Building a Successful Cloud Financial Management Practice
- Building a Successful Cloud Operations and Governance Practice
- Building a Successful Cloud Infrastructure Security and Compliance Practice

Item No: 17031065aq-wp-glbl-asmt-cld-mgmt-matry-uslet 9/23