# MAVEN WAVE'S GUIDE TO BUILDING THE FOUNDATION FOR SUCCESS IN THE CLOUD

INNOVATION-DRIVEN DIGITAL TRANSFORMATION

## AUTHORS

**Jason Foa**
Managing Director, Cloud Infrastructure

**Shannon Rush**
Principal, Cloud Architect

**David Zhu**
Principal, Cloud Architect

Phone: + 1 312-883-9254

Email : jason.foa@mavenwave.com
Website: www.mavenwave.com

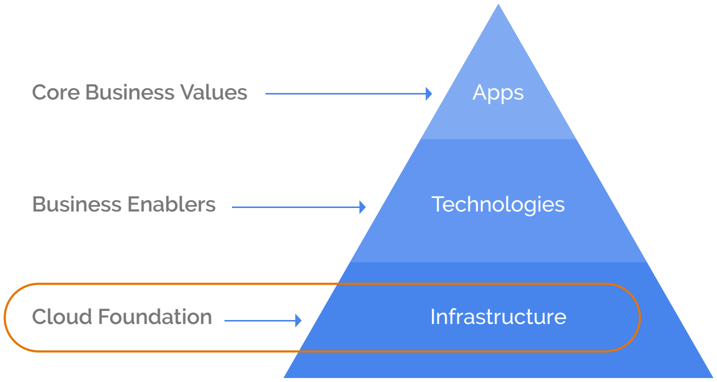
# MAVEN WAVE'S GUIDE TO BUILDING THE FOUNDATION FOR SUCCESS IN THE CLOUD

If you haven't already moved at least some of your workloads to the cloud, you are likely considering it and weighing the pros and cons of being in the cloud. There are countless reasons to migrate to the cloud, but one stands out among the rest: **in almost all cases, it's cheaper.**

This cost savings allows your IT department to free up budget away from vital functions, such as keeping the lights on, so that you can focus on the initiatives you want to undertake, such as creating a strategic advantage for your business. The other primary reason to migrate to a cloud infrastructure is to open up a whole new toolbox of capabilities, such as machine learning and advanced analytics afforded by cloud providers like Google and Amazon.

**But how do make sure you're getting started on your journey to the cloud the right way?**

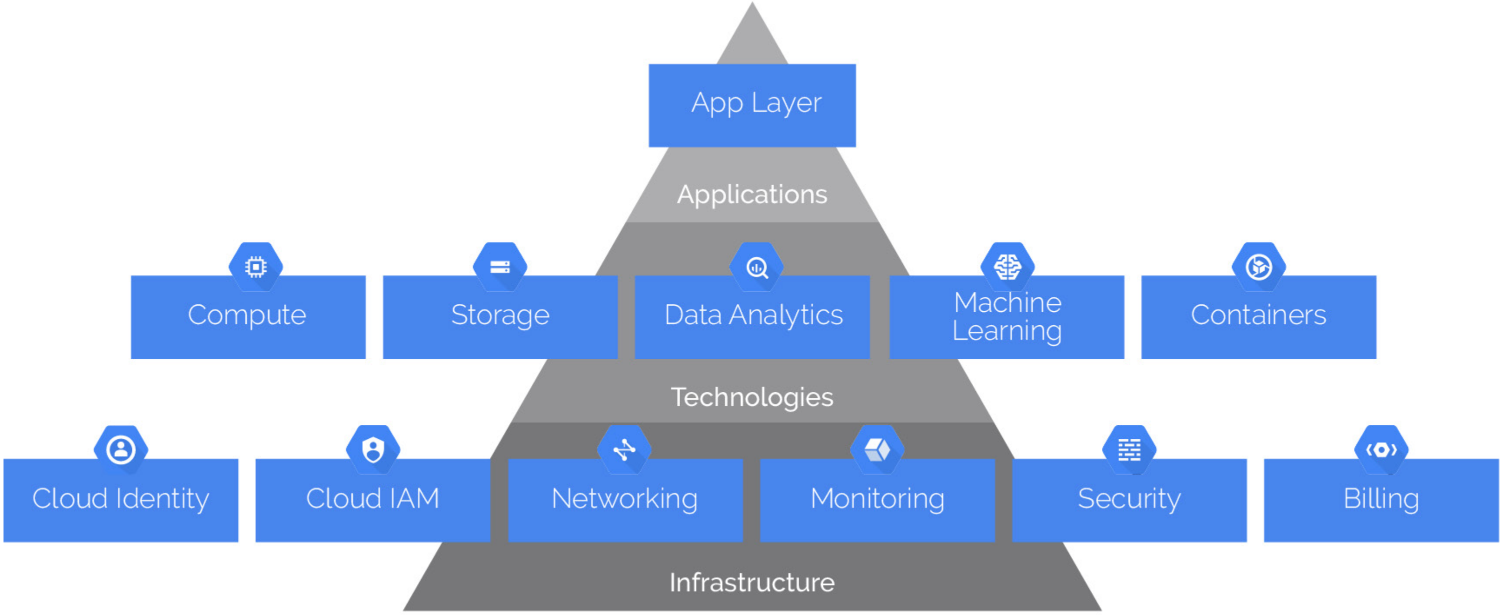
At Maven Wave, we use the metaphor of building a house to communicate what needs to be done to realize the benefits of the cloud. Just as a solid foundation is a critical component to any building, infrastructure is the foundation for success in the cloud.



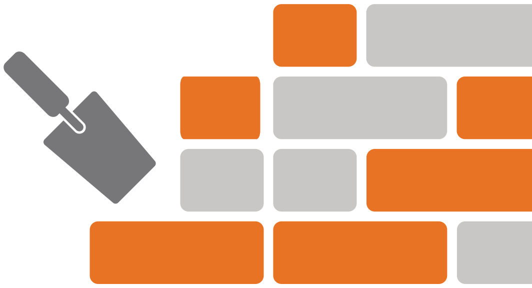
You need this solid foundation to reduce your costs and overhead as well as to empower your team to use cloud native tools. In this article, we will focus on the six critical elements of building the cloud foundation and our tips for setting your business up for success:

1. Establishing identity
2. Granting access
3. Monitoring
4. Allocating costs through billing
5. Connecting to network
6. Security to protect the environment.

While this article discusses Google Cloud Platform (GCP) as the tools in the descriptions of these six elements, the concepts can be applied to AWS, Azure, or any public cloud.



# MAVEN WAVE'S GUIDE TO BUILDING THE FOUNDATION FOR SUCCESS IN THE CLOUD



## Establishing Identity

To start building your foundation, consider how your users will be established with an identity on the GCP platform. The ease of set-up is one of the best aspects of the platform; all it requires is a Gmail account and a credit card to get started. However, this ease can also be a double-edged sword because those short-cuts can propagate through your environment. It's important to ensure people aren't using non-managed Google accounts to access your environment.

If you're using G Suite, your enterprise directory is already being synced to Google. As your cloud deployment scales, it's important to make sure users are properly grouped according to their responsibilities. Groups make privilege management much easier, so you don't have to assign individual users to roles. But keep in mind that in G Suite, groups are intended to be constructs for mailing lists. On the GCP platform, these groups can drive up costs, so it's a critical step to review your groups and which users have the ability to create groups.

## Granting Access

Now that we've established identity, we will focus on providing access to cloud resources. Similar to the way you should always bundle users in groups, you should always group projects in folders. Your folder hierarchy can be based on application environment (prod, test, dev) or on business function. Regardless, it's important to be thoughtful about how your hierarchy is designed and to base it on how you would like to aggregate permissions. Otherwise, you may end up with a spaghetti plate of permissions as your environment grows. As in other environments, apply the principle of least privileged access; users should have access to perform their job functions and nothing else.

One note of caution: Google is constantly evolving the platform, and they update the predefined roles accordingly. So if you have an administrator assigned to the predefined Compute Editor role and Google adds a new feature to the Google Compute Engine (GCE), your admin will still be able to perform the same functions that they could before the introduction of the new feature. But if you've defined a custom role for administration, Google will not update the privileges of your custom role. As such, you should use custom roles sparingly. Finally, for high-impact roles, such as project creator and billing administrator, identify three people with overlapping responsibilities to ensure appropriate coverage during vacations or in the event of attrition.

## Monitoring

Most IT organizations are comfortable monitoring operational metrics, such as uptime and utilization. With the cloud, you need to make sure you're monitoring consumption as well. You're only going to pay for what you use, but you're going to pay for everything you use. If that usage spirals beyond your expectations, your costs will too. Organizations need to establish a cloud monitoring function that's separate from the project ownership. Copy the log to a different bucket/project, with a different owner, as part of a gsutil or cron job.

Tools like Google's Stackdriver Monitoring provide enhanced monitoring of your resources and alerts. Create a cloud monitoring project and everytime you spin up a new project, create a new Stackdriver account and use a dedicated project to house all Stackdriver accounts for purposes of non-repudiation. If Stackdriver or other monitoring tools have a separate account per project, permission management can get complicated.

Storing logs in Google's BigQuery costs the same as Cloud Storage - with that cost being cheap - and provides a platform for analyzing logs and deriving additional insights into how your GCP implementation is being used as well as which uses are driving cost.

## Billing

As discussed in the previous section, the reason that monitoring consumption is important is simple: consumption drives costs. Billing is how you allocate those costs. Cloud platforms provide a great deal of billing detail that can help you allocate costs more effectively within your organization. Organizing your resources into folders provides the additional benefit of having another level of billing rollup.

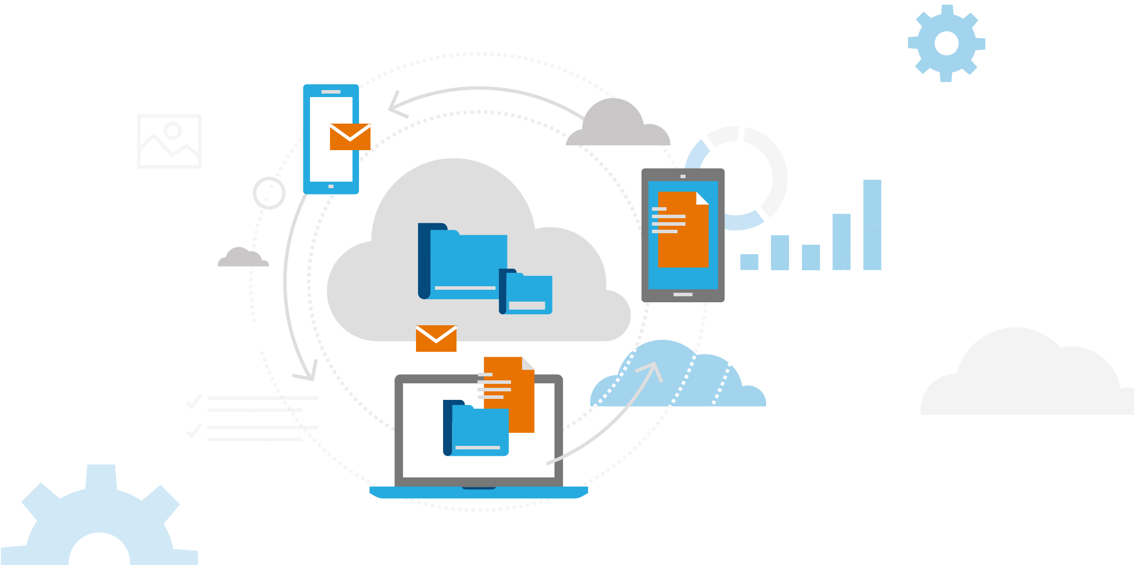
As you spin up VMs, you'll have an idea of how much each application and folder will likely cost you. But sometimes, whether it's due to a poorly designed query or a spike in traffic on your website, costs can exceed your expectations. To prepare for this possibility, make sure that you configure a monthly threshold for each billing account. Note that this is not a cap on the spend for the billing account. Instead, it is a monitoring mechanism. Billing administrators receive notifications when the account reaches 50%, 90%, and 100% of this monthly threshold, but Google won't make a decision for you to shut down or throttle spend.

## Networking

Networking is the foundational element of establishing connections from your cloud environment to your on-premise environments, other clouds, and the public internet. Similar to the way you want to grant permissions to groups based on the principle of least privilege, you should use networks and subnetworks inside of projects to isolate groups of similar VMs based on the principle of least privilege.

Enable private access to Google managed services and platforms where available. This will force network traffic onto the Google backbone versus out to the public internet. Keeping your traffic on GCP's (or another provider's) network reduces egress charges and eliminates potential points of security risk.

Additionally, use network tags rather than an implicit IP address whenever possible. Network tags are text attributes you can add to virtual machine (VM) instances. Tags allow you to establish firewall rules and routes applicable to specific or groups of VM instances. Similar to the way you want to isolate your network edges in a traditional network, create a dedicated project for your internet edge networks to reduce the blast impact of a security breach.
Google provides a currently unique configuration capability that allows you to establish a shared Virtual Private Cloud (VPC). The VPC provides a console that allows you to manage multiple regions and zones from one place as well as centralizes network and security management. With a shared VPC, your networking group can allocate one set of IP addresses. If you want to create an IP address scheme, you don't need to create IP addresses and subnets for every project. Project owners can attach anything they want to subnets that have been shared by the VPC owner. Because it's so important, create a dedicated VPC host project for your shared VPC to keep it secure.



# MAVEN WAVE’S GUIDE TO BUILDING THE FOUNDATION FOR SUCCESS IN THE CLOUD

## Security

Security is the sum of the precautions and safety measures you put in place to protect your implementation. The most important factor of security to keep in mind is that you need to be vigilant. The biggest risk to any cloud deployment is not inherent in the technology, but instead in the user community, whether that’s a disgruntled former employee, an easily-guessed password, or a workstation left unlocked.

That said, Google and other cloud platforms do provide some technologies to help keep your environment safe. Use Google integrated authentication through gcloud, with two-factor authentication, and the console to protect boxes. Google will handle security and just-in-time creation of accounts inside of Identify Manager. The less than ideal alternative is creating accounts and managing keys as you would with a local VM in your data center. If you are publishing assets on the internet, but still want to isolate access, use Cloud Armor to employ white-list/black-list methodologies to shape inbound traffic. You can also use IAP to force Google authentication in front of any web application that you’ve published, but users need to have a Google group/login. Any security you have on your Google account is now applied to web applications.

## BUILDING THE FOUNDATION

Whether you’re planning a migration to the cloud to save money or to introduce new capabilities to your business, you want to make sure you’re building your infrastructure on a solid foundation. At Maven Wave, we can help you build that strong foundation for a cloud architecture that will set you up for success in the cloud, enabling you to build up your technology stack and deploy applications with ease.

Cloud computing provides business benefits, but planning a migration or identifying the right solution can get complicated, fast. Maven Wave helps clients work through challenges at any stage, on any of the major public cloud platforms or multi-cloud environments.

Contact us to get started!

## AUTHORS

**Jason Foa**
Managing Director, Cloud Infrastructure

Phone: + 1 312-883-9254

Email : jason.foa@mavenwave.com
Website: www.mavenwave.com

**Shannon Rush**
Principal, Cloud Architect

**David Zhu**
Principal, Cloud Architect