# AWS, Azure, and GCP: Account Setup Instructions

Note, these instructions are subject to change as each cloud provider opts to improve or change their registration process and user experience.

## Amazon Web Services (AWS)

Here are the basic steps to set up an AWS cloud account:

1. Go to aws.amazon.com and click on "Create an AWS Account".
2. Follow the prompts to set up your account. You'll need to provide contact information, create a username and password, provide payment information like a credit card, and go through identity verification.
3. Choose the type of AWS support plan you want. The Basic plan is free, Developer and Business plans start at $29/month. You can upgrade later.
4. Once your account is created, you'll be taken to the AWS Management Console. This is where you can access all the AWS services.
5. As a security best practice, create an IAM (Identity and Access Management) administrator user for yourself instead of using your AWS root account for daily work.
6. Secure your root account credentials like access key ID and secret access keys. Don't share these keys or check them into code repositories.
7. Set up multi-factor authentication (MFA) on your root account and admin IAM accounts for added security.
8. Configure a billing alarm to monitor your usage and avoid unexpected charges.
9. Start using core AWS services like EC2, S3, VPC, etc by referring to the user guides and documentation. Consider getting certified in AWS.
10. Monitor your infrastructure using CloudTrail, CloudWatch, config rules etc. to ensure security, availability and optimize costs.

## Microsoft Azure

Here are the typical steps to set up an Azure cloud account:

1. Go to azure.microsoft.com and click on "Start free" to create your account.
2. Provide your email and phone number to receive a verification code. Enter the code to validate your identity.
3. Fill in your profile information - name, email, account type (personal, business, etc). Agree to the Azure Customer Agreement.
4. Create a username and password for authentication.
5. Add a payment method such as credit card to enable paid services later. You'll need to provide card details even for the free tier.
6. Select your country/region. This will determine your data residence and which Azure data centers you can access.

7. Choose your preferred subscription - Free trial, Pay-as-you-go, or Member offers if applicable. The free trial gives you $200 credit for 30 days.
8. Start using Azure services! The common starting points are to create resources like virtual machines, storage, databases, etc.
9. Monitor your usage on the Azure portal dashboard. Set billing alerts and quotas to manage costs.
10. For security, use Multi-Factor Authentication and Role-Based Access Control to manage permissions.
11. Analyze Azure Advisor recommendations to optimize performance and costs.
12. For compliance needs, evaluate tools like Azure Policy, Security Center, and Azure Monitor logs.

## Google Cloud Platform (GCP)

Here are the typical steps to set up a Google Cloud Platform (GCP) account:

1. Go to cloud.google.com and click on "Get Started for Free" to begin creating your account.
2. Sign in with your Google account if you have one, or create a new Google account. This will be the root account for GCP.
3. Provide your contact information and agree to the GCP Customer Terms of Service.
4. Select your country and preferred billing currency.
5. Add a payment method such as credit card. This is needed even for the free trial.
6. Choose your GCP project name. Projects allow you to organize GCP resources.
7. Enable APIs and services like Compute Engine, Kubernetes Engine, Cloud Storage etc. that you want to use.
8. For security, ensure 2-step verification is enabled on your root account.
9. Create service accounts with limited privileges and use them to access GCP instead of the root account.
10. Allocate project roles like Administrator, Viewer etc using IAM permissions.
11. Start deploying resources like VM instances, containers, databases etc within your project.
12. Monitor usage through dashboards, logs and alerts to avoid unexpected costs.
13. Use tools like Security Command Center, VPC Service Controls, Cloud Audit Logs for security and compliance.

Use these steps to get started with AWS, Azure, or GCP. If they change, feel free to contact me, and I will be glad to update this reference.