

WHITEPAPER

---

# The Art of Landing Perfect on Cloud - Part I



# Contents

<b>Introduction</b>	<b>04</b>
<b>Importance of Landing Zone</b>	<b>05</b>
<b>Challenges</b>	<b>06</b>
<b>Landing Zone Planning</b>	<b>07</b>
Who are the stakeholders?	07
Which cloud platform?	08
What to deploy?	09
Which region should host your workloads?	12
Cloud native or agnostic?	13
Single-account or multi-account structure?	15



# Executive Summary

Adopting the Cloud is one of the highest priorities of almost every organization and industry in today's IT world. Thousands of organizations have adopted the cloud-first approach where any IT application is evaluated for hosting on cloud first.

A cloud deployment journey starts with a comprehensive landing zone setup, known as Day 1 in the cloud. Landing zones serve as virtual data centers in the cloud, providing essential infrastructure components. Strategic planning involves addressing challenges like stakeholder engagement, platform selection, and organizational structure. Cloud platform selection should consider application portfolio and TCO comparison. Deployment planning covers organizational units, identity management, security, monitoring, and governance. Region selection involves factors like compliance, latency, and service availability. Choosing between cloud-native and cloud-agnostic services depends on workload distribution and requirements. A multi-account structure offers advantages in isolation, budgeting, security, operations, innovation, and service quotas. A well-planned landing zone is crucial for successful cloud adoption, ensuring scalability, security, and alignment with organizational goals.

# Introduction

Organizations are increasingly adopting cloud solutions for their scalability and security benefits. This whitepaper sheds light on the key aspects of a successful cloud deployment strategy, emphasizing the importance of a well-planned landing zone.

A landing zone is one of the steppingstones of a cloud foundation. It enables organizations to establish the foundational services and processes to onboard the applications and resources on cloud in an accelerated and efficient manner. In this whitepaper, we are going to understand the importance of a cloud landing zone, the challenges you face while planning for it, what needs to be planned for and finally how to plan it.

Your cloud journey starts with assessing the readiness for cloud adoption followed by the landing zone setup in cloud, also called Day 1 in cloud. Assessment and Planning for the applications to be migrated, if any, can run in parallel to the landing zone setup. **The landing zone design and deployment is a three phased approach, namely:**



**Design and Plan**  
(Day0)



**Deployment**  
(Day1)



**Operations**  
(Day2)

# Importance of a landing zone

A landing zone is a well-architected multi-account setup (virtual data center) in the cloud, with all baseline infrastructure applications and services. These include networking, security, monitoring, backup, user and account governance, ready for hosting and operating applications in the cloud. This is a starting point for your organization to launch and deploy workloads and applications in the cloud quickly and confidently.

By engaging the right stakeholders, you ensure that the cloud adoption is not hurried but planned well, addressing everyone's concerns and ideas. It allows you to onboard and have all the stakeholders' consensus before any deployment on the cloud.

Developers must know how essential services are designed and deployed on the cloud and the governance policies to follow. It helps them design applications so it is easier for cloud engineers and architects to run and maintain those applications in the cloud.

Cloud landing zones reduce the preparation time significantly, which in turn reduces the migration time of applications. For example, creating a new account/subscription for migrating an application on the landing zone can happen within minutes, along with all the baseline configurations. Your governance policies can automatically be extended to new accounts with the right configuration.

# Challenges

Since landing zones are the foundation of your cloud environment, it is crucial to think carefully and strategize what you want to build in the landing zone and how. Here are some questions you must have before creating a landing zone.

- Who should participate in the landing zone planning?
- Which cloud platform to opt for?
- What should be deployed in the landing zone to make it ready for hosting applications?
- Which region(s) hosts the workloads in the cloud? Should it be a multi-region or a single-region approach for production and disaster recovery workloads?
- Should we go with cloud-native services for everything or cloud-agnostic applications?
- What should be the org structure in the landing zone?
- How do you plan networking design and connectivity with on-premises and branch networks?
- How much network bandwidth would we need for hybrid connectivity and backup options in case of an outage??
- How do you implement identity and access management in the cloud?
- What security controls should we begin with?
- What governance policies should we begin with?
- What financial controls should we begin with?

# Landing zone planning

This section will explain how to plan a landing zone in the AWS cloud. However, most of it can also be applied to other cloud providers by incorporating their technical differences.

## Who should participate in the landing zone planning?

Building a landing zone involves technical and business decisions across account structure, networking, security, operations, governance, and access management. Your organization's growth and business goals for the future are also taken into account.

The landing zone for every organization varies depending on their structure, size, requirements on the cloud, etc. Therefore, there is no fixed way for an organization to structure its landing zone. However, the building blocks remain the same for every organization and industry.

It would be best to start by creating a core working team from different departments in your organization. Include IT (Cloud and Enterprise Architects), Business Strategy, Finance, Security (Identity management and Security architects), Application (Enterprise Application Architects), Network (Network Architects) etc. This team will work collectively to brainstorm the design of the landing zone.

## Which cloud platform?

Next, you identify the right target cloud for your organization. Understand the current application portfolio in your organization today and identify the software and tool stacks they are leveraging. Try to identify the patterns here, **for example:**



**Do you have a Microsoft-heavy stack (Windows servers vs. Linux servers, MS SQL databases vs others)?**



**Do you have more containerized applications than fixed-capacity ones?**



**Look for sample case studies or reference materials for complex workloads hosted on the cloud. For example, ERP solutions, AI/ML solutions, etc.**

Also, consider the target application portfolio based on your organization's plans, **for example:**



**Are you planning to modernize the applications by SaaSifying or PaaSifying them during the cloud migration?**



**Are you planning to undertake the cloud-first approach, where new applications are designed for the cloud (using the 12-factor approach)?**



**Do you plan to undertake the serverless approach or server-based approach?**

Do a thorough TCO comparison of your target workload in the cloud. You must also compare each cloud platform based on the above pointers and identify the right fit for your organization's needs.

If your workload contains data bound by local regulations, selecting a cloud provider with a region in the respective geography will override all other evaluation factors.

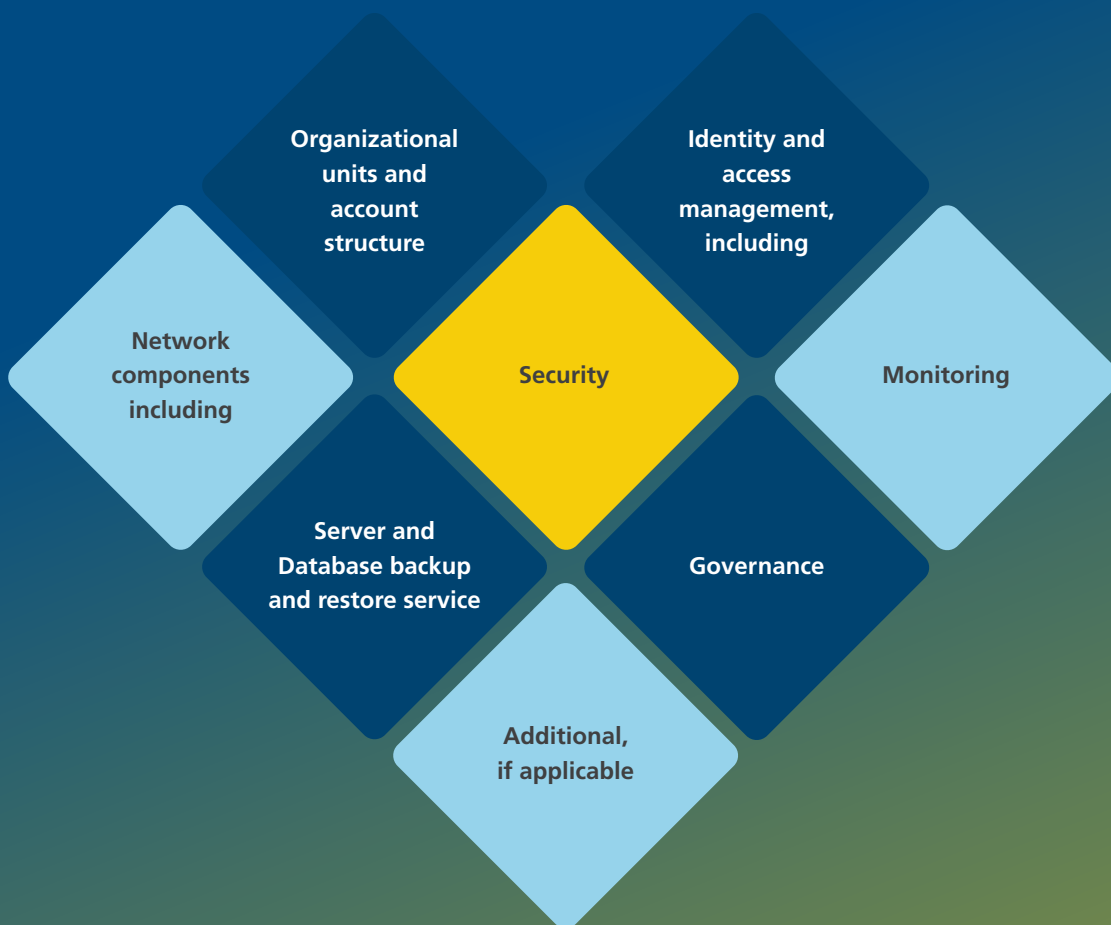


## What to deploy?

Once the core team is established and you have identified the right cloud platform, it is time to start planning the cloud landing zone.

As explained earlier, a landing zone is a virtual data center in the cloud, with all the baseline infrastructure applications and services for hosting and operating applications.

You need to start planning the following applications, services, and controls at a minimum.



## 01 Organizational units and account structure

---

## 02 Identity and access management, including

- Identity federation
  - RBAC controls
  - Default users, groups, and permissions to be created
  - Multi-factor authentication
- 

## 03 Network components including

- VPC/VNET along with subnets, route tables, gateways, etc.
  - Network connectivity between VPC/VNET, Accounts / Subscriptions
  - Connectivity between on-premises and cloud network
  - Private connectivity between cloud resources and services (endpoints)
  - DNS
- 

## 04 Security

- Preventive and detective controls
  - Network firewall, Web application firewall, DDoS protection
  - Cloud security posture management
  - Security information and event management (SIEM)
  - Activity events collection from the cloud platform
  - Advanced threat detection
  - Antivirus
  - Vulnerability management
  - Patch management
  - Bastion hosts
  - Data encryption keys/services
  - Password policy for local users
-

## 05 Monitoring

- Operating system and application performance
  - Network and security monitoring
- 

## 06 Server and Database backup and restore service

---

## 07 Governance

- Tagging policies
  - Accounts and resource naming convention
- 

## 07 Additional, if applicable

- DR environment infrastructure
  - CI/CD and DevOps toolsets
- 

You may not need to deploy everything simultaneously based on what you plan to host/migrate to the cloud and when. You may not need certain components until a certain stage to host the workload in the cloud. For example, setting up a WAF (Web Application Firewall) may be postponed in two scenarios. Either your internal applications don't need firewall security, or the workloads ready for migration don't include external applications.

## Which region should host your workloads?

Generally, cloud computing resources for all cloud providers are hosted in multiple locations worldwide. These locations are called Regions, Availability zones, and Local zones.

Every cloud provider has its construct of regions and availability zones. Some of them group multiple availability zones into a single region while others may call a single datacenter an availability zone. Generally, an availability zone is a group of multiple data centers with redundant power supply, network, etc., in a specific geographical area.

Some considerations that may help you decide the regions and availability zones are listed below.



### Compliance

If your workload contains data that is bound by local regulations, selecting a region that complies with the regulation overrides other evaluation factors.



### Latency

User experience is key for any organization. Consider the latency users may face while accessing the workloads in the cloud. Choosing a region close to your users' base location can reduce the network latency.



### Availability zones

Some of the regions may have fewer availability zones than others. There are some regions in certain cloud platforms with only one availability zone. Choose an availability zone based on your business needs, whether multiple or limited.



### Service availability

Some cloud services may not be available in certain regions. Evaluate the cloud services you foresee using immediately or in the near future.



### SLA

The cloud providers may offer different SLAs in different regions.



### Cost

The charges for some services are higher in certain regions than others.

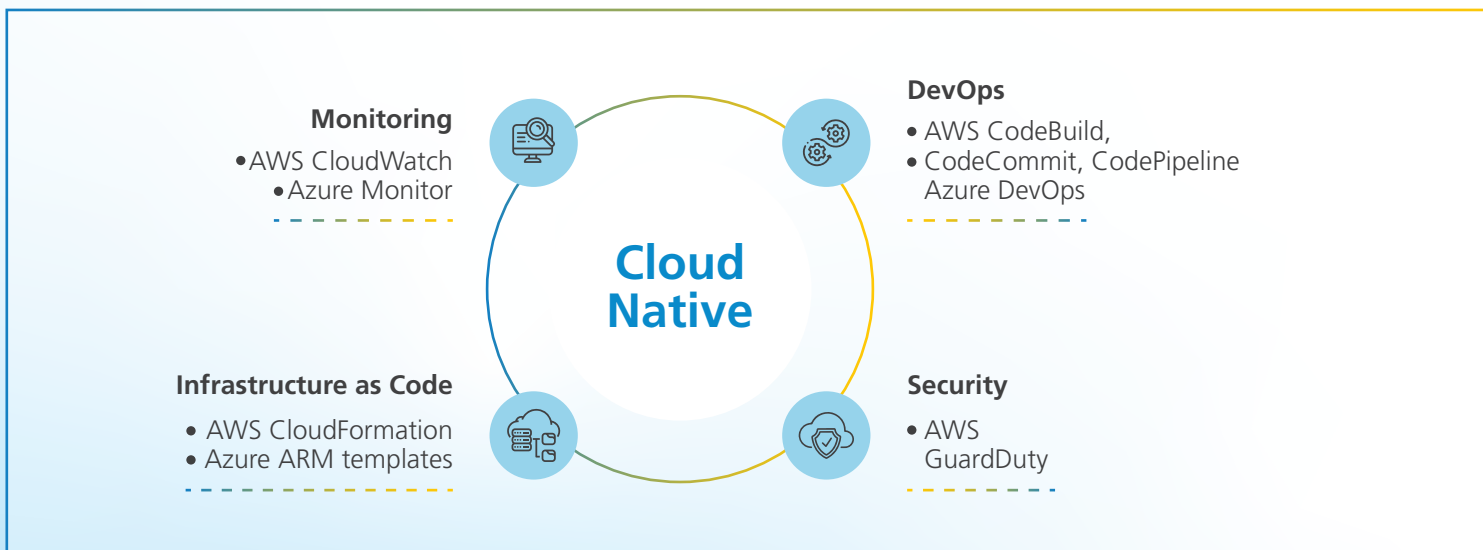
## Cloud-native or agnostic?

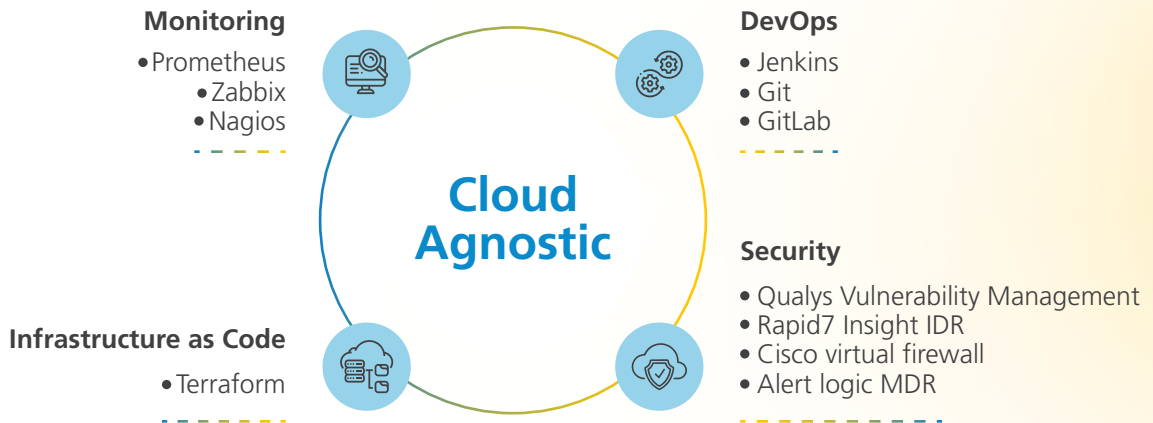
The next stage is the technical planning for your landing zone. One of the important questions is whether to go with cloud-native services or third-party cloud-neutral services. This is a much-debated question, and everybody has their point of view on it.

Cloud providers offer cloud-native services for creating and managing resources. On the other hand, cloud-agnostic services provided by third-party software providers support operations across multiple public and private clouds and, to an extent, on-premises workloads.

Cloud-native services are built primarily for the same cloud platform and are best compatible with resources hosted within. They can also support certain operations across cloud platforms or on-premises workloads but with limited capabilities. Cloud-native services also offer the advantage of new features and capabilities being released by the cloud provider. On the other hand, cloud-agnostic services may have fewer features at a given point in time. This is because they rely on the availability of features and support by cloud-native services to an extent by leveraging the APIs of the cloud-native services.

Here are some examples of cloud-native and cloud-agnostic services.





As explained above, cloud-native services provide the best compatibility and more features for services in the same cloud platform and, therefore, are a good fit. On the other hand, cloud-agnostic services offer more flexibility, good compatibility, and features for services in multiple clouds and on-premises workloads. You need to weigh your options on the following criteria:

**01** Is your workload spread across a single cloud or multi-cloud?

If it is multi-cloud or even hybrid-cloud, cloud-agnostic services are more suitable. They offer a centralized management platform and visibility without your teams having to learn about multiple tools and technologies for the same operation.

**02** What are your requirements and expectations with each service? What do you want to do and achieve with it? Does it support them?

## Single-account or multi-account structure?

Have you thought about how the workloads will be distributed in the cloud? Do you want to host everything in the same account or spread across multiple accounts for better isolation?

Distributing the workloads across multiple accounts has some advantages.

### 01 Better isolation

You can group workloads for a common business unit or purpose in a single account. It can help you align the ownership and decision-making for each account and avoid conflicts and dependencies with workloads in other accounts.

### 02 Budgeting and credits

The multi-account approach can help you with budgeting and financial management better. Each business unit in your organization can have a defined IT budget that they must adhere to. They can also have clear visibility of the current vs. the forecasted spending. I have seen, some business units in large organization connect directly with the cloud providers and making purchases. They make their purchases for credits, discounts, and plans. Purchases and discounts meant for one unit cannot be used by other business units.

### 03 Security

It is easy to restrict access to a certain part of the workload for application and business teams with a multi-account approach compared to a single-account environment.

The surface area in the event of a security breach can be greatly reduced in a multi-account setup with appropriate controls in place.

## 04 Operations and governance

Business units or product teams in your organization may have different processes. Isolation of business units can help them operate with greater control but still provide overarching guardrails.

Different security control requirements for production and non-production environments can be easily managed with a multi-account approach.

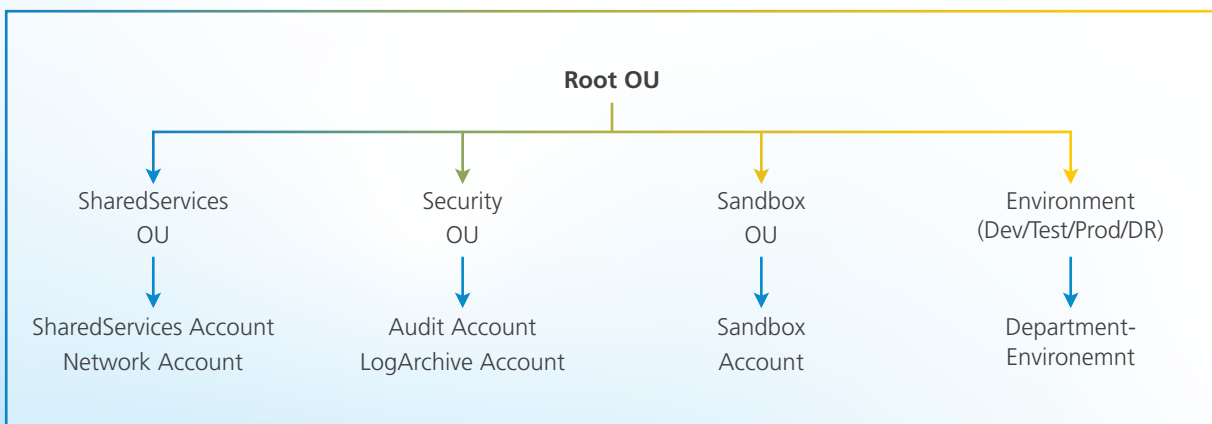
## 05 Innovation

Your product teams can have a separate account in the cloud for any new development or proof of concept in isolation from the actual production and non-production environment.

You can still re-use some existing applications and services, ensuring the required isolation from the IT environment. For example, single sign-on is possible without network connectivity to the IT environment.

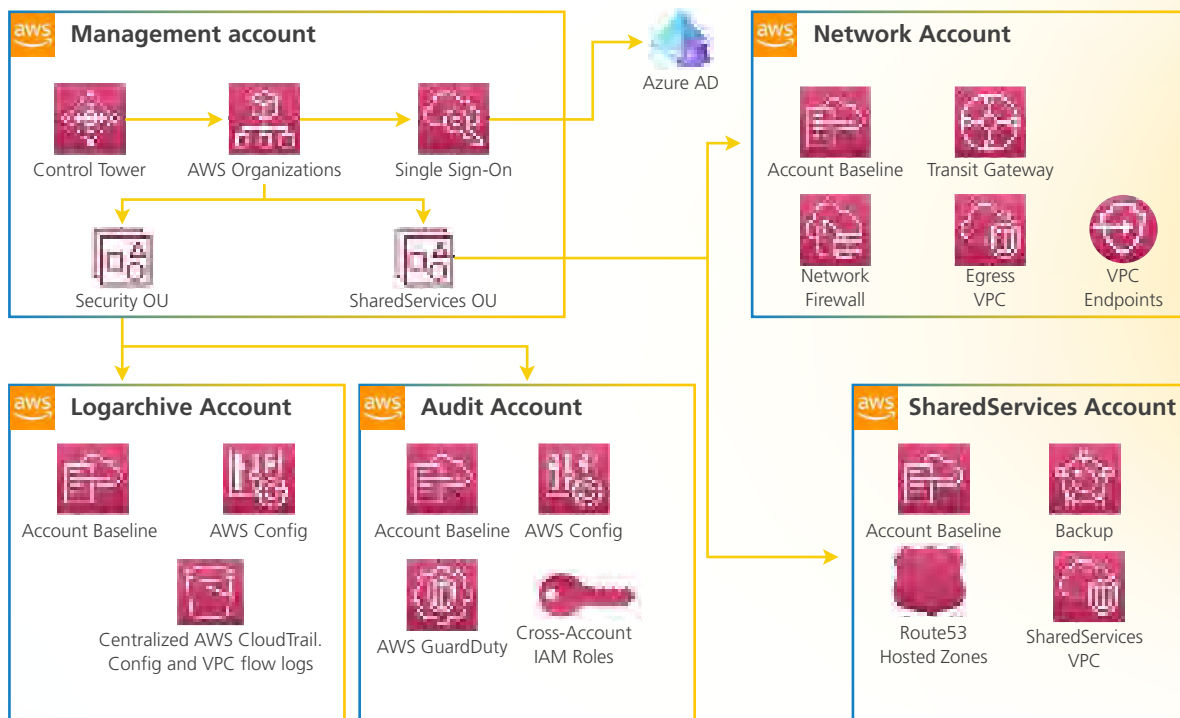
## 06 Service quotas

Every cloud provider has some soft and hard limits for their services. A multi-account setup can help you overcome those limits with appropriate solutions.



Sample Organizational Unit Structure





I highly recommend the multi-cloud setup over a single account, especially in the following scenarios:

- If your organization is starting its cloud journey, it is good to have things that help you govern and manage things better and support your organization’s growth in the future.
- If you have a cloud-first strategy, having a foundation that gives you more control over things makes more sense.
- If you plan to run a significant workload in the cloud.
- If you are a mid- or large-sized organization with plans to use the cloud to its optimum advantage.

Single-account setup can be a good fit if:

- You are only doing some testing to see how the cloud fits into your organization's strategy.
- You are a small organization with a lesser number of workloads that can be hosted in the cloud.

# Conclusion

Cloud adoption is a top priority, with organizations embracing a cloud-first approach. In this whitepaper, we saw that a well-planned landing zone is crucial, serving as a multi-account setup for secure cloud deployment. Engaging stakeholders, understanding cloud-native services, and strategic planning are key. The phased approach of Day 0, Day 1, and Day 2 ensures a structured cloud journey. Challenges include platform selection, region choices, and the cloud-native vs. cloud-agnostic debate. A multi-account setup is recommended for scalability and control. In essence, a thoughtfully designed landing zone is fundamental for confident and efficient cloud adoption. In the next part, we will see how to design identity and access management, network connectivity, security and financial controls, and governance policies. We will also learn about landing zone deployment, validation, and best practices.

We'll continue the discussion for the remaining part of landing-zone planning in [Part 2](#) of this whitepaper.

## Author



**Gaurav Goel**

Gaurav Goel is an IT professional with over 15 years of experience in Cloud Architecture, Cloud Consulting, DevOps, Infrastructure as Code, System Administration, and many other roles. He has worked with clients from various industries, such as Telecom, Retail, Oil and Gas, Utility, Manufacturing, Education, etc. Gaurav is a technology enthusiast who likes learning new technologies and sharing knowledge with others.



**LTIMindtree** is a global technology consulting and digital solutions company that enables enterprises across industries to reimagine business models, accelerate innovation, and maximize growth by harnessing digital technologies. As a digital transformation partner to more than 700 clients, LTIMindtree brings extensive domain and technology expertise to help drive superior competitive differentiation, customer experiences, and business outcomes in a converging world. Powered by 82,000+ talented and entrepreneurial professionals across more than 30 countries, LTIMindtree — a Larsen & Toubro Group company — combines the industry-acclaimed strengths of erstwhile Larsen and Toubro Infotech and Mindtree in solving the most complex business challenges and delivering transformation at scale. For more information, please visit <https://www.ltimindtree.com/>