Cloudscaler®

A Guide to Landing Zones

HOW TO ENABLE CLOUD SUCCESS

We've been successfully using landing zones to support enterprise-scale transformation for over 10 years. In this guide we share some of our learnings to help you get the most effective landing zone possible. One that underpins cloud success.

How did we get here?

So why do landing zones even exist? Where did they come from?
The advent of cloud and its inherent characteristics in terms of being easy to spin up cloud resources quickly led to 'cloud chaos' – organisations found themselves with a multitude of environments, inconsistent governance and risk mitigation, technology sprawl, and spiralling cloud spend. Landing zones evolved to solve some of these problems whilst also retaining all the inherent benefits of cloud. The reasons you're using it in the first place. A landing zone enables you to use it more efficiently and effectively.

Let's start with a definition.
What actually is landing zone? A landing zone is the foundation for a centralised cloud platform. It is the infrastructure layer between a hyperscaler and the business applications you're building and operating. It provides common cloud standards, tooling, and services to mitigate the risks of running cloud-based production services also making it easier and faster for teams to adopt cloud. It not only simplifies cloud use across your organisation – it enforces standards, tooling, and services, enforcing the risk stance of your organisation.

Using a landing zone, you can:

// **Simplify the use of cloud,** making it faster and easier for delivery teams.

// **Embed and enforce standards** across security, data, operations and spend.

// **Mandate preferred tooling,** reducing technology sprawl.

// **Reduce duplication** across delivery teams by providing pre-approved tools and services.
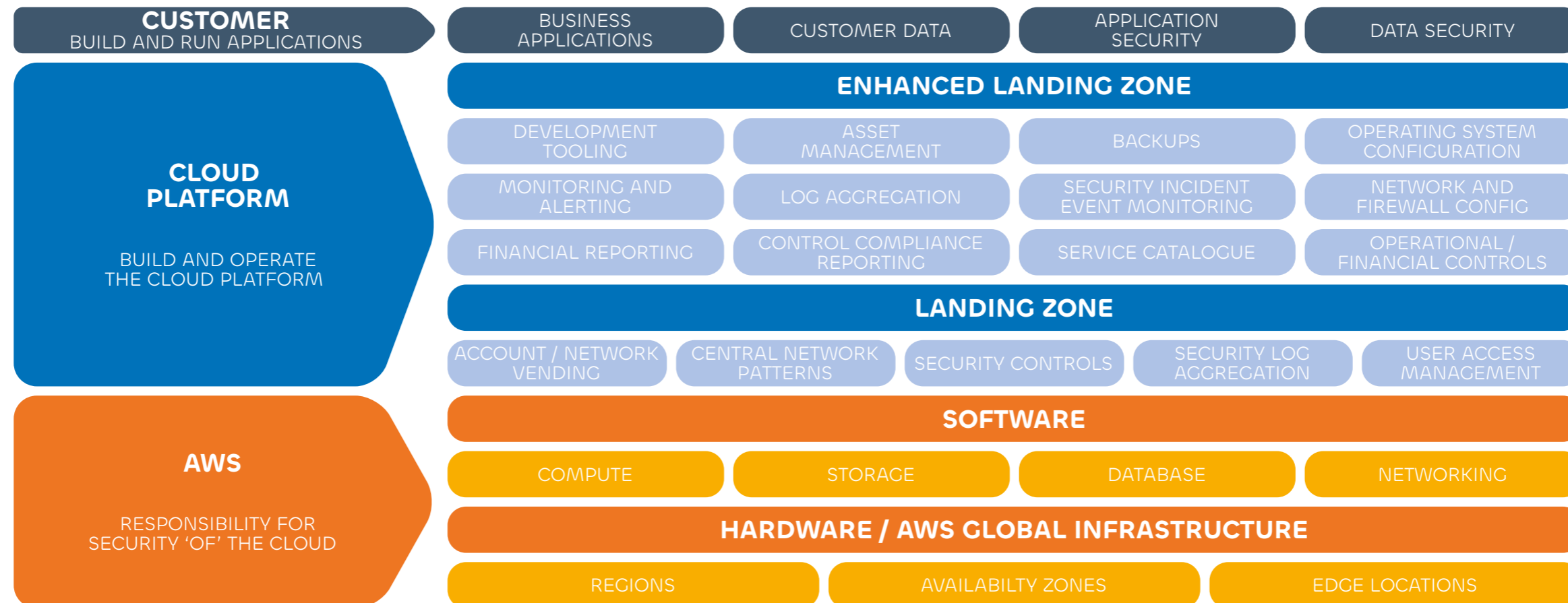
Why a basic landing zone isn't enough

How do you build a landing zone?
Option 1

You can opt for some of the landing zone options offered by the hyperscalers. AWS has Landing Zone Accelerator, Azure has a landing zone portal accelerator, Google has Secured Landing Zone. These options enable you to effectively 'press a button' to deploy a landing zone in minutes. All the basics done for you but also kept up-to-date so you don't need to pay to do the maintenance yourself.

Do you have to do anything before pressing that button or need any specialist skills to press the button? Most definitely, because not only are there landing zone variants for industry verticals, but every landing zone service available has configuration options which will significantly alter the way in which your landing zone will operate. Before you can use any of the public cloud providers landing zone services, you need to follow best practice and define your objectives,

scope, and requirements. There will be fundamental technical decisions you'll need to take care of as well. You'll need to know what to do once that landing zone is live. Don't forget you'll also need to define a cloud operating model and cloud governance framework, to include your internal shared responsibility model. See our checklist below for a full run down of what you should do before going anywhere near 'that button'.

CUSTOMER BUILD AND RUN APPLICATIONS	BUSINESS APPLICATIONS	CUSTOMER DATA	APPLICATION SECURITY	DATA SECURITY

	ENHANCED LANDING ZONE			
CLOUD PLATFORM BUILD AND OPERATE THE CLOUD PLATFORM	DEVELOPMENT TOOLING	ASSET MANAGEMENT	BACKUPS	OPERATING SYSTEM CONFIGURATION
	MONITORING AND ALERTING	LOG AGGREGATION	SECURITY INCIDENT EVENT MONITORING	NETWORK AND FIREWALL CONFIG
	FINANCIAL REPORTING	CONTROL COMPLIANCE REPORTING	SERVICE CATALOGUE	OPERATIONAL / FINANCIAL CONTROLS

LANDING ZONE				
ACCOUNT / NETWORK VENDING	CENTRAL NETWORK PATTERNS	SECURITY CONTROLS	SECURITY LOG AGGREGATION	USER ACCESS MANAGEMENT

	SOFTWARE			
AWS RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD	COMPUTE	STORAGE	DATABASE	NETWORKING

HARDWARE / AWS GLOBAL INFRASTRUCTURE		
REGIONS	AVAILABILTY ZONES	EDGE LOCATIONS

So, you've done all the preparation work and 'pressed the button'. Is it a workable landing zone that you can instantly start migrating workloads to? Probably not. Services like AWS Landing Zone Accelerator provide a basic landing zone which is likely to only be suitable for non-critical or pilot workloads. To use it for anything more advanced than Development you'll need to tailor it and layer additional controls and tooling according to your specific requirements and risk appetite. How much tailoring you need to do will vary according to your size, scope and resources/skills – for example, the sector you operate in, the regulatory landscape you're subject to or the cloud services you wish to make available via your Service Catalogue.

Option 2. BYO

You can build your own landing zone.
Then surely you will have implemented a landing zone which is perfect for your organisation? Not in our experience. Doing it yourself tends to see clients embark on a journey of exploration filled with trial and error – one that takes far longer to achieve a fully-functional landing zone and incurs significant cost. In fact, when we talk to those who have taken the BYO route, we find they:

// **Take much longer** to complete the build and when they finally think it's ready, they have significant technical debt plus their teams have become frustrated with the wait and started work in their own environments in the meantime. Those teams tend to be reluctant to change what they're doing and start to use the shiny new landing zone. Just because you've built it, doesn't mean they will come.

// **Never finish.**
As they're building their landing zone, new services and external threats are evolving - as soon as one element is in place, it is out of date so they're constantly playing catch-up. Business pressure means interim solutions are put in place to meet demand, diverting resources away from the build. Or their scope and specification is just too big or ambitious.

// **Think it's fit for purpose when it's not.**
Going into build mode too quickly can mean you're not using best practice or keeping up with technological advances. You'll be confined by the skills and experience of your in-house resource. When we have looked under the hood of landing zones that the owners proclaim to be perfect, we have found it's not running as it should, isn't following best practice and isn't ready for critical workloads.

// **Struggle to get regulatory approval.**
We have seen a number of organisations spend a significant amount of time and money building their own landing zone only to fall at the final hurdle – regulatory approval. They're not able to make any workloads live. They've invested in a platform that they can't use and are still paying for their legacy solution. Not only that, they have resources dedicated to the build and operation of infrastructure they can't use. Costs are high plus key stakeholders start to lose confidence and get frustrated by delays.

So, what is the best approach? We'll take you through the key steps to success.
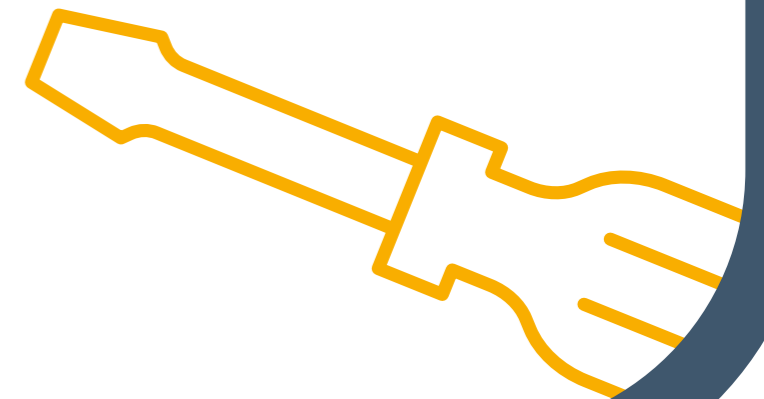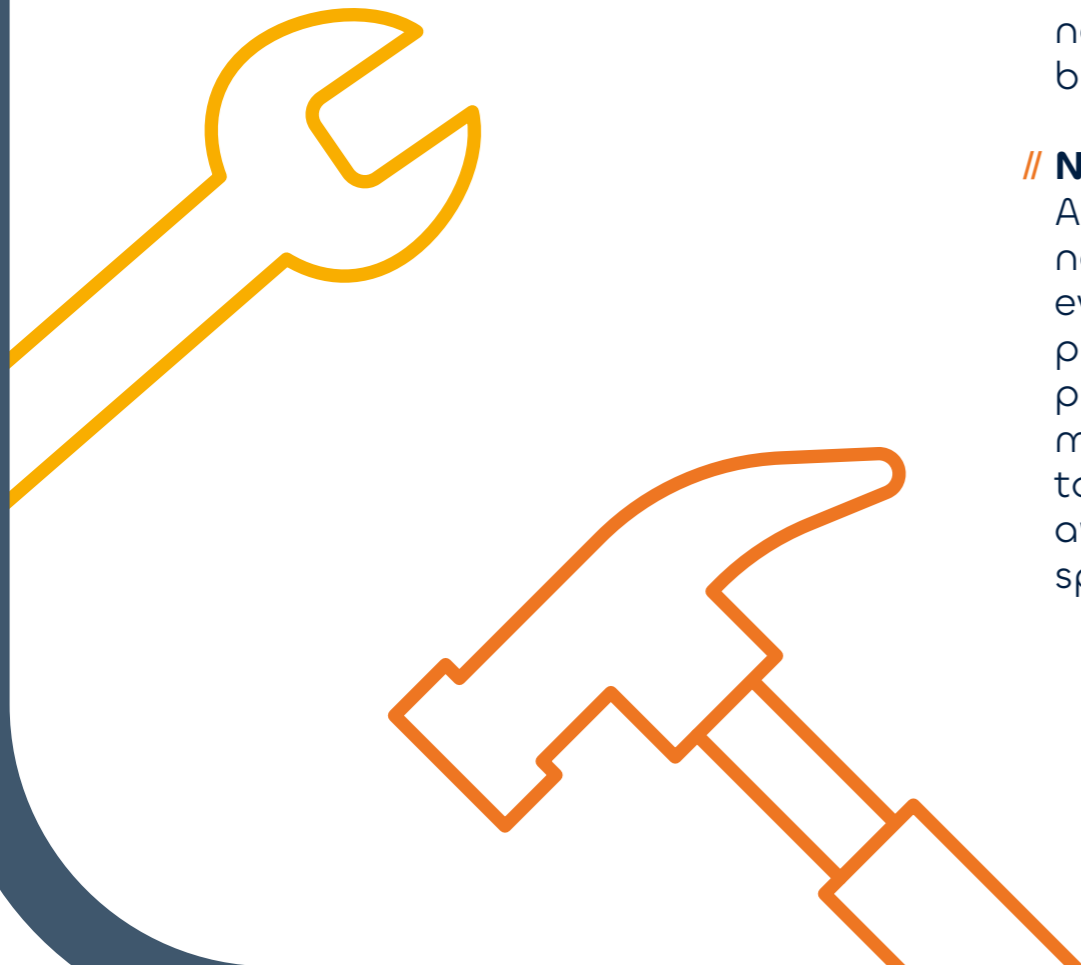
Get the basics right first

Before using a landing zone service, or if you have already built your own, make sure you:

// **Have a clearly defined cloud operating model and cloud governance framework**, to include your internal shared responsibility model. How will accounts be provisioned. Consider account structure in terms of production, development, testing, and shared services accounts. Your cloud operating model will also need to consider who will be accountable for prioritising new landing zone features as well as building out, maintaining, and supporting the landing zone.

// **Have the right skills in place** to not only deploy the landing zone service (if you're using one) but to then manage and develop your landing zone (as defined by your cloud operating model).

// **Assess current state.**
Take a thorough look at your existing infrastructure, applications, and processes. Identify any gaps, limitations, or areas that need improvement in terms of cloud readiness, security, compliance, scalability, and performance.

// **Determine scope and requirements.**
Consider factors such as the number of accounts, regions and workload types that will be included as well as the compliance requirements that your landing zone needs to meet.

// **Design the architecture.**
This will need to include the account structure, network topology, identity and access management (IAM) policies, security controls, logging, and monitoring mechanisms. You'll need to check your architecture follows best practice and meets all your requirements.

// **Network ready.**
You'll need to agree the networking patterns and high-level network design.

// **Establish security controls.**
These will need to span network security, data encryption, threat detection, and identity management. It may require security groups, virtual private clouds (VPCs), firewall rules and secure communication channels.

So, you've got the basics right, what next?

Get a head start

We strongly advise you against building your own landing zone. Deploying a proven landing zone product from your chosen public cloud provider will mitigate many of the risks associated with running production workloads in the cloud. These services offer a fast-start solution which could save you months, or even years, of effort as well as a significant amount of money.

Plan for the future

Using a proven landing zone product makes it easier and quicker to plan for the future.

You'll need multiple instances of your cloud platform - as a minimum we recommend Dev, Test and Live versions.

These different implementations enable you to build and test new landing zone features after you've gone live to ensure they're proven and ready to deploy. With multiple landing zone implementations, you can do this without disturbing users.

The people aspect

You'll need to **train and educate stakeholders.**

// **Provide training and education** to key stakeholders, including IT teams, developers, and business users.

// **Promote awareness** of best practices, security considerations, and operational processes to ensure successful adoption.

// **Involve your teams** in the development and test phases, take them with you on your transformation journey. Most importantly gather their feedback throughout – during build but also after any enhancements.

// **User experience and feedback needs to be positive.** Your landing zone needs to provide a good user experience to be truly successful. It needs to be a business enabler, not a blocker.

Tailor to suit
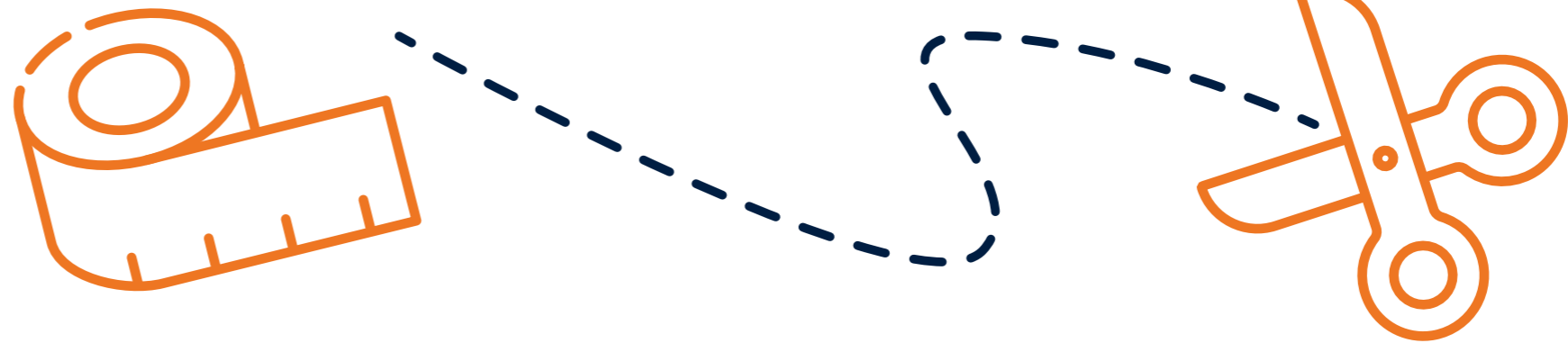
You may have deployed your chosen landing zone service or have built your own initial version. This provides a Minimum Viable Platform (MVP) – what we call a base landing zone. A starting point. This starting point may be good enough to deploy pilot workloads to.

However, to migrate workloads with higher risk profiles, you will need to tailor or enhance it to ensure it is fit for purpose. You'll need an enhanced landing zone.

Why you need an enhanced landing zone

If a landing zone enables you to get from A to B in cloud terms, think of that MVP landing zone as a bicycle. It will get one or two workloads from A to B. But it won't get them there particularly quickly or provide them with ultimate protection. What you want to do is add an engine, leathers and a helmet as well as a sidecar.
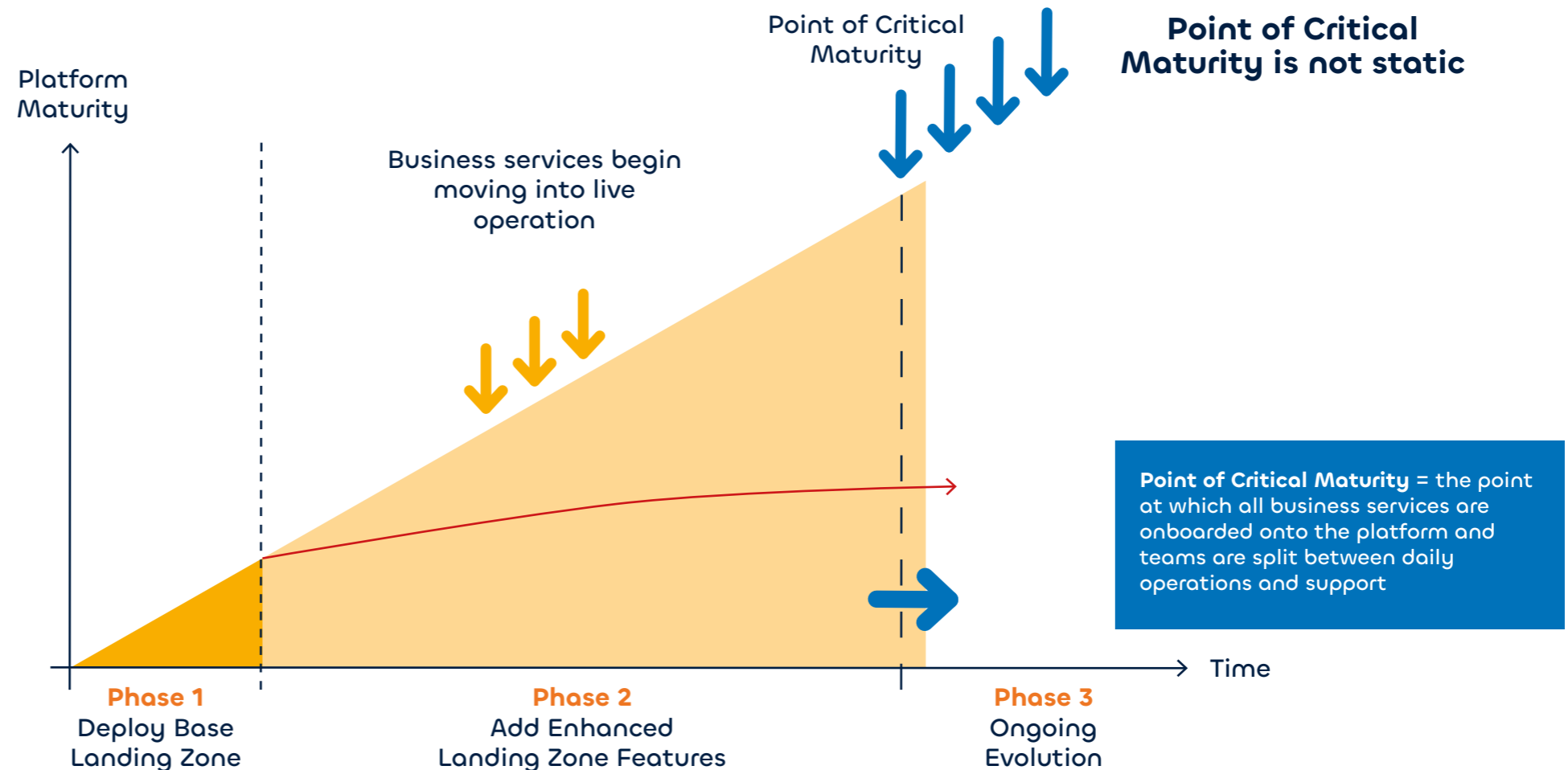
You'll need to amend and add to the controls provided by that MVP landing zone to provide the levels of risk mitigation that are appropriate for your size, your threat landscape, your regulatory requirements. You'll also need to create an opinionated (wrapped) version of services (i.e. a Service Catalogue) available to tenants. Doing so will ensure they adhere to best practice which in-turn will ensure consistency.

So, here's your checklist of what you need to enhance your MVP landing zone:

☑ **Development Tooling**
CICD pipelines, container image repositories and scanning, centralised secrets management solution, testing capabilities (chaos engineering, load and performance testing).

☑ **Asset Management**
Data catalogue, data classification and tagging.

☑ **Backups**
Automated backup, secure backup vault and access policies.

☑ **Operating System Builds**
Hardened/tooling enhanced OS build repository. Supported policy and monitoring.

☑ **Monitoring and Alerting**
Set up monitoring and logging mechanisms to ensure visibility into the performance, health, and security your landing zones and the applications using it. If you're using AWS, you'll want to utilise services like CloudWatch, AWS Config, and AWS CloudTrail to capture and analyse relevant logs and metrics.

☑ **Log Aggregation**
Centralised logging account for secure log storage; application, security, VPC Flow and CloudWatch logs shared with the appropriate teams; archive and retention policies in line with regulation.

☑ **Security Information and Event Management (SEIM)**
Monitoring and alerting configured for all appropriate events, with relevant monitoring tooling, logs, on call rotations and escalation paths clearly defined and accessible.

☑ **Networking and Firewall Configuration**
Central patterns defined and clear and efficient processes for firewall configuration management. Automated creation and management of networking resources as part of the account vending pipeline.

☑ **Financial Management and Reporting**
Strong governance via detailed resource tagging and anomaly tracking. Scheduling and cost efficient solutions (instance right sizing, reserved capacity planning and usage, appropriate technology selection – e.g. spot instances). Cost management integrated into account creation and platform controls (e.g. cost centre tagging, instance type restrictions)

☑ **Control Compliance Reporting**
Monitoring of controls and centralised reporting of compliance, both for teams and for management. Tracking of historical compliance and alerting on regression

☑ **Service Catalogue**
Central catalogue of common services, provided with baseline configurations that are compliant with policy to accelerate delivery and increase conformity while reducing churn and technical debt. Over time the scope can increase from simple service modules to reusable complex systems e.g. load testing frameworks or packaged business solutions.

☑ **Operational Controls**
Code management, release processes, CICD management, automated deployment and rollback, live service monitoring and reporting, smoke tests for common processes (e.g. Account creation, destruction)

Don't forget if you've got the basics right and the right people in place, enhancing your landing zone should be pretty straightforward. A clearly defined cloud operating model and governance framework will be essential.

Plan for evolution

Platform Maturity

Point of Critical Maturity

Point of Critical Maturity is not static

Business services begin moving into live operation

Point of Critical Maturity = the point at which all business services are onboarded onto the platform and teams are split between daily operations and support

Time

Phase 1
Deploy Base Landing Zone

Phase 2
Add Enhanced Landing Zone Features

Phase 3
Ongoing Evolution

The key thing to remember is your landing zone will never be 'done'. You can't just walk away. Think of it like painting the Forth Bridge. Once you finish, you have to start again.

Yes, you built a landing zone that met the requirements of your initial workloads but now you need to develop the landing zone to meet the requirements of more critical workloads. You also need to update it to keep up-to-date with best practice and service developments. **Your landing zone needs to evolve over time.** You will then need to adopt a phased migration plan that is synchronised with the evolution of your landing zone.

Once again, if you have a sound operating model and governance framework in place, they will underpin and define how your landing zone evolves over time.

Don't forget to allow for proper testing, validation, and user acceptance before migrating critical systems. Establish a process for onboarding new applications and workloads onto the Landing Zone framework. Again, this should be covered by your cloud operating model.

As part of your phased migration, you can prioritise the deployment of critical components and gradually expand the Landing Zone framework to cover additional accounts, regions, and workloads.

Continuously optimise and iterate. Regularly review the Landing Zone framework, assess its effectiveness, and identify areas of improvement. Wherever possible, leverage native tools and services to continuously optimise costs, enhance security, and improve operational efficiency.

Conclusion

Congratulations. You're on the right path if you've decided to deploy a landing zone, or you already have one. To ensure that landing zone quickly delivers value and innovation to your business you need to:

// **Build your foundation first.** Your operating model, governance and people.

// **Get an MVP landing zone live as soon as possible.** Use pilot workloads to demonstrate how effective the landing zone is in order to secure confidence and ongoing investment.

// **Enhance that MVP to suit higher risk profiles.**

// **Adopt an agile approach** to enhancing your cloud platform. Implement the most critical aspects for your users first and then continue to iterate with regular releases containing new features and improvements. Gather feedback. Ensure a positive user experience.

// **Implement a phased migration plan** that is synchronised with your platform evolution.

How we can help

1. **Optimise an existing landing zone.**
   If you have a landing zone, but unsure about it, our Cloud Confidence Check will identify opportunities to enhance and optimse it.

2. **Validate your build plan.**
   Before you start your build, we can review your plans, check them against best practice and identify any potential issues or opportunities to improve.

3. **Team augmentation.**
   We can provide additional resource to plug any skills gaps or ensure your teams can focus service delivery not infrastructure.

4. **Operating model and cloud governance model support.**
   We can help you define, refine or improve these two cloud essentials.

5. **Landing Zone build, optimisation and support.**
   We offer fast start landing zone service bundles if you want an enhanced landing zone live in under 2 weeks. We can also optimise, enhance or support an existing landing zone.

Get in touch to discuss how we can help you. www.cloudscaler.com/landing-zones

Why Cloudscaler

// We know landing zones. It's what we do.
We're approved AWS Landing Zone Accelerator partner, and a founding member of the AWS LZA programme. We don't try to be all things to everyone. We specialise in the build, optimisation and management of AWS cloud platforms.

// We've done it before.
We have extensive experience in the delivery and optimisation of AWS cloud platforms for organisations such as the Home Office and Santander. You benefit from our knowledge of best practice.

// You can trust us.
We're trusted by customers in highly-regulated sectors such as UK Public Sector and Global Financial Services. They trust us and so can you.

// Speed.
We can mobilise our AWS experts within hours to start work on your solution.

// Assured procurement.
We're ProServ Ready which means you can contract Cloudscaler through AWS, and if you're a public sector organisation you can engage Cloudscaler through the relevant CCS frameworks.

Get in touch to discuss how we can help you.
www.cloudscaler.com/landing-zones