expertthinking

Landing Zones

Core principles to consider when building cloud landing zones

HELPING YOU ACHIEVE MORE. FAST.

AZURE & AWS CLOUD EXPERTS.

www.expert-thinking.co.uk | team@expert-thinking.co.uk | +44 (0) 333 050 3331

Expert Thinking (Consulting) Limited, a company registered in England and Wales, company number 10716331, whose registered office is Camburgh House, 27 New Dover Road, Canterbury, Kent, CT1 3DN, and whose principal mailing address is The Gridiron Building, 1 Pancras Square, King's Cross, London, N1C 4AG.

About the Author: Alex Brightmore

Expert Thinking Principal Consultant, experienced in building enterprise cloud platforms and developing cloud strategy at scale.

For more information, please contact:

Emma Pegler

emma.pegler@expert-thinking.co.uk

+44 (0) 7730 164857

What is a Landing Zone?

Landing Zone is a modular foundation for cloud workloads - the platform to build out your cloud estate. Landing Zones encompass security controls, governance, core networking, infrastructure, and identity.

They provide a platform to onboard and accelerate migration, modernisation and innovation.

However, there is more to it than just deploying your Infrastructure as Code.

To accelerate cloud adoption and avoid the many potential pitfalls of moving to the cloud, strategy, people, process and operating models all come into play.

The technical foundation must be strong to enable seamless onboarding, compliance, security and fast realisation of business value.

Maturity is a journey, which this whitepaper will detail, pointing out the many "gotchas" along the way.

Technical Considerations

Defining the cloud hierarchy is vital as it allows for segregation and controls to be layered.

Landing Zones should be developed and managed as code. Managing infrastructure manually is not viable or strategic for secure, maintainable and mature cloud platforms.

This should be delivered to environments via CI/CD, with controls for critical environments (such as production), testing wrappers and reusable pipelines.

Building up the security posture of a Landing Zone starts with identity and cloud controls.

Managing identity and access to environments and resources, while enabling self-service and innovation, is a vital part of Landing Zone design.

Cloud controls form the framework to which Landing Zones and workloads are governed, what is and isn't permitted across the cloud estate, and policy-based guardrails to enforce security controls and configuration.

Design Considerations

Design for the business needs, building in capability to scale and change as the business evolves. This includes everything from access management to repeatable modular architecture and code solutions.

Consider process and consumption from the start. How will consumers of your Landing Zone onboard quickly, to deliver value and achieve more, fast.

Embed the architecture function to your design process, extending to consumers. Minimum rules of engagement should apply to any current and future workloads. Ensure requirements are properly scoped, key design decisions captured and maintained over time and design standards are set.

Be flexible and fluid, cloud is ever evolving with new tools, technologies and standards. Design review should be regular and adding in additional capability to your Landing Zone should be a key part of your strategy.

Starting the Journey: Foundations & Strategy

Building a successful Landing Zone requires technical expertise and strategic direction - know your skills gaps! Building secure and scalable network infrastructure is the core of any Landing Zone.

Defining how this is consumed and maintained over time is paramount.

Whether it is 'Hub-And-Spoke', flat hierarchy or a single workload, getting the foundations right sets the organisation up for growth and consumption.

Consider everything. From centralising core platform resources (logging & monitoring, network ingress/egress) to how teams across an organisation consume cloud services, leave no stone unturned.

Address people and process from the start. Whether they are engineers, stakeholders, project managers, or technical leads, bring everyone on the journey to support successful Landing Zone builds.

Collaborate, collaborate, collaborate. Breaking down silos and barriers between teams is a crucial success factor.

The Do's & Don'ts

- Do be agile! Iterate, fail fast, and deliver incremental change to build the Landing Zone right.
- Do leverage Infrastructure as Code. A well-designed codebase with replicable environments is an accelerator, not a blocker.
- Do establish a governance baseline. What critical security measures should the business implement via policy? What should consuming teams be enabled to do?
- Don't adopt cloud and build in isolation. The organisation's strategy and business needs should drive change.
- Don't lift and shift controls and legacy on-prem security policies to the cloud and expect them to stick. Cloud requires a rethink of how to approach security and consumption of services.
- Don't solely focus on the Landing Zone build and the tech. People need to know how, why and what, so establish a clearly defined operating model.

Developing:
The “Ops”, Governance & Security

"The Ops"; CloudOps, DevOps, FinOps.

Each of the "Ops" is an operationalising of process and technology to enable automated, streamlined and observable delivery to cloud.

Regular releases to environments, centralised controls and governance, and controlling costs across workloads are part of "The Ops" maturing.

Building the skills internally required for cloud maturity.

CloudOps gives cloud consumers a governance and service consumption layer, defining the method of onboarding and controls across Landing Zones.

DevOps methodologies facilitate cohesive, fast and secure methods of building repeatable code assets into cloud Landing Zones.

FinOps is the operationalising of cost. Assigning budgets, controlling resource sizing and SKU, reporting, showback and chargeback.

Governance & Security

- Do adopt a cloud controls framework, such as the Cloud Security Alliance Framework.
- Do segregate networks and apply perimeter controls to subnets via network security rules.
- Do adopt policy controls aligned to the above to regulate the configuration of resources (for example, blocking public network access or automatically deploying default network rules).
- Don't give everyone elevated access. Manage identity and access as a first-class security control.
- Don't bundle everything into single environments. Logical separation reduces blast-radius. Don't rely on the Cloud Service Provider to encrypt your data and traffic - be proactive.
- Don't open up firewalls in the cloud to speed up delivery. Define the right rulesets and iterate as consumption increases

Policy Control Examples

✗ Public Network access should be blocked	→	✓ Deny deployment of open NSGs/Resources
✗ VM size should be restricted for cost	→	✓ Whitelist usage of a sub-set of all SKU's
✗ Logs should be gathered by default	→	✓ Deploy-if-not-exist s diagnostic settings
✗ Usage of services should be restricted	→	✓ Whitelist only Business approved services
✗ There should be an audit trail	→	✓ Audit access logs & activity logs

Onboarding:
Business Value, Automation & Scale

So, you have a well-architected, secure Landing Zone ready to be consumed by teams. What now?

The separation of "Platform" and "Workload" is essential. Access controls and policy controls should protect centralised services such as core virtual networking and firewall configuration.

Vending consumer environments should be automated in code, with guardrails applied by default.

Minimum rules of engagement: Adopt a "you build it, you run it" mindset for consumers.

Core touchpoints like network peering, diagnostic settings and RBAC should be automated in code as part of a standardised vending process in your Landing Zone.

Create reusable templated code for resource usage and CloudOps maintained service catalogues. This way, consumers can move fast and deliver business value.

Maturing:
Monitoring & Maintenance

- As your Landing Zone and the people/process capabilities wrapping around it mature, 'Design Authority' comes into focus.
- A Design Authority is a centralised function to review workload proposal, architectural designs, services to be consumed and security controls against solutions.
- The intention here should be to ensure the Landing Zone guardrails and best practices are carried through the whole cloud estate.
- Your Landing Zone should cater for any consumer workload, from customer- facing applications to internal data APIs.
- Unlike a data platform, application environments may have different service requirements and controls applied to them.
- Iterate via the CloudOps capability and build a service definition catalogue with associated policy controls in place.

Monitoring & Maintenance

Observability is a critical part of resiliency and auditing across Landing Zone environments.

Leverage cloud native tooling to automatically log, monitor and alert to security events, audit access, and monitor compute performance. Encompass all workloads onboarding to the cloud.

Allow consumers to self-serve logs and metrics while proactively monitoring the overall cloud platform posture.

Landing Zones should evolve and mature as cloud adoption increases; don't let things stand still.

Cloud services develop over time. This may be new functionality or features, additional security protocols or even deprecation of certain features.

The same goes for Infrastructure as Code. Keep evolving your code in line with version updates and new functionality. Don't get left behind!

In Summary

- Landing Zones are the foundations to deliver business value, they are critically important in your ability to maximise benefit from cloud
- Security and governance are core pillars of design and should be given appropriate thought and consideration from the very start
- Consider the people, process, and operating model elements in just as much depth – ways of working drive lasting value and benefit
- Develop Landing Zones in code, deliver via CI/CD
- Keep iterating the Landing Zone – cloud does not stand still, and neither should your teams
- Enable consumers to move quickly and deliver value safely – guardrails are an enabler, not a blocker

For more information, please contact:

Emma Pegler

emma.pegler@expert-thinking.co.uk

+44 (0) 7730 164857