Safe Landing Zones for Enterprise Migrations
Introduction

Many traditional IT vendors and systems integrators treat the shift to public cloud as an evolution of traditional data-center server migration. Using decades old thinking and processes around security, networking, operations, and deployment can greatly impact the speed to value of your cloud migration project.

These traditional lift & shift mass migrations into the cloud often happen without thinking through the best operational and governance approaches to manage the environment over the long-term. The lack of detailed planning in these areas frequently leads to rework, longer migration timeframes and higher ongoing costs for management of your cloud.

Turbot believes that public cloud (IaaS and PaaS) presents a clear transformational shift for Enterprise IT. This change requires a new approach for operations, planning, migration, and service transition of cloud platforms; including new skills and tools for the teams executing the change. The result of this transformation will be an IT organization dedicated to the principles and practice of Software Defined Operations (SDOps) as the new way of working with their Software Defined Infrastructure.
Maximizing Value from Application Isolation

One of the key “new ways of working” in public cloud is the principle of application isolation, which is best achieved through a well-architected and controlled multi-account strategy. For large enterprises (especially in regulated industries) Turbot recommends deploying separate production and non-production accounts for each business service; by doing so, the organization gains extraordinary benefits:

**Cost Savings / Transparency:** Ability to associate 100% of specific cloud costs to a specific application workload, environment, cost center, or business unit. Can use account service limits to impose restrictions on a business unit, development team, or project.

**Administrative isolation between workloads:** Administrative isolation by account provides the most straightforward approach for granting independent administrative groups different levels of administrative control over cloud resources based on the workload, development lifecycle, business unit (BU), or data sensitivity.
Limit visibility and discoverability of workloads: Accounts provide a natural boundary for visibility and discoverability. Workloads cannot be accessed or viewed unless an administrator of the account specifically enables access.

Isolation to minimize blast radius: Separate accounts help define boundaries and provide natural blast-radius isolation; this provides a mechanism for limiting the impact of a critical event such as security breach or account suspension.

Strong isolation of recovery and/or auditing data: Businesses that are required to control access and visibility to auditing data due to regulatory requirements can isolate their recovery data and/or auditing data in an account separate from their workloads (e.g., writing AWS CloudTrail logs to a different account), or ensuring logs are maintained only in specific regions.

Safe Landing Zone Approach

The benefits of isolation through the multi-account model yield even greater value for large-scale migration of applications. When planning and testing migrations, it is critical that application teams have access to network isolated environments that allow them to test end-to-end functionality of their application without fear of data corruption or duplicative web-service/API transactions happening during testing and prior to application cut-over.

Turbot’s Safe Landing Zone approach gives the cloud team the ability to stamp out repeatable patterns of migration account landing zones for dev/test and production instances. Each application team gets full access to deploy and test their application in their own landing zone and through that process discover and document the approach for production cut-over.

In this model, teams can choose the migration approach (e.g. lift-and-shift, re-platform or re-architect) that works best for their application, without worrying about stepping on permissions, configuration or networking from other workloads. The approach also creates a clear shared-accountability model between the enterprise cloud team and the application migration teams, allowing for federation of the work necessary to execute on migrations; this avoids a common issue of the expert cloud team becoming a bottleneck for an enterprise migration while they troubleshoot individual application architectures.

Guardrails for Landing Zones

Turbot guardrails are the cornerstone technology that allows repeatable and consistent starting points for safe landing zones. Guardrails ensure data protection and security for the enterprise, accelerating and simplifying cloud capabilities for the migration teams,
and giving each application team the ability to safely modify policies for the localized needs of their workloads.

Turbot’s robust hierarchical policy engine gives the enterprise control at higher levels of the hierarchy, and the flexibility to create exceptions for migration workloads on an account by account basis (or even at the resource level). This resolves much of the friction that is caused by “one-size fits all” models that are typical of cookie-cutter models.

As part of the migration process, Turbot will work with the cloud, networking and security teams to identify repeatable and automated guardrail settings for your migration based on the workload and regulatory/compliance needs of your company.

Some key examples of how Turbot guardrails can specifically be used to accelerate and ensure success of your migration program:

**Services Whitelist:**
- Specify whitelisted cloud services based on workload types (e.g. GxP, HIPAA, PCI)
- Enforce least privilege and discovery of application needs by requiring that teams explicitly turn on the services they need as part of the deployment and testing processes.

**Network & Firewall Management:**
- Application isolation; automate consistent and secure network constructs and security groups for predefined patterns (e.g. DMZ, intranet only, sandbox)
- Enforce lockdown of network and security groups to foster best practices, isolate workloads and foster discovery of network usage
- DNS record management through customer defined schemes
- Automate and enforce “north-south” and “east-west” firewalls
Identity and Access Management:
- Consistent identity management across AWS, Azure, GCP, OS, DB, Turbot & SaaS
- Full stack audit trail of user activity
- Active Directory & SAML integration
- Federation of application teams access across multiple organizations
- Time-limited privilege grants to maintain segregation of duties
- Secure audit trail of all activities, permissions grants and guardrail changes
- Simple point & click user interface to grant and track access

![Image](image.png)

Grant `<USER> <LEVEL> rights for <SERVICE> on resources in <SCOPE>.

- Owner = Manage access
- SuperUser = All changes; and
- Admin = Med-High risk; and
- Operator = Low-Med risk; and
- ReadOnly = Read data; and
- Metadata = Read metadata; and
- User = Basic access, no rights

Operating System, Database & Data Protection:
- Enforce use of specific AMIs and AMI publishers
- Enforce use of specific DB engines
- Enforce enterprise security hardening (e.g. CIS) on VM images
- Enforce custom application specific configurations
- Manage OS users, groups, and SSH keys
- Manage DB users, groups and passwords
- Automate snapshot and data retention policies
- Automate and enforce implementation of encryption policies

Cost Management:
- Budget-setting for migration test accounts
- Cost allocation & show-back for application migration testing
- Auto-stop instances on a schedule
- Clean-up unallocated volumes, log & snapshot rotation
About Turbot

Our mission at Turbot is to unlock the value of public cloud for enterprises through innovation, insight and speed. Turbot has built a strong brand and reputation by hiring the right people, continually innovating and enhancing the product, and providing unparalleled customer service.

Contact Us

Email: info@turbot.com
Twitter: @turbothq
LinkedIn: https://www.linkedin.com/company/turbot
Phone: +1 973 922 0297
Address: https://turbot.com

Turbot HQ, Inc
1732 1st Ave #20232
New York, NY 10128 USA