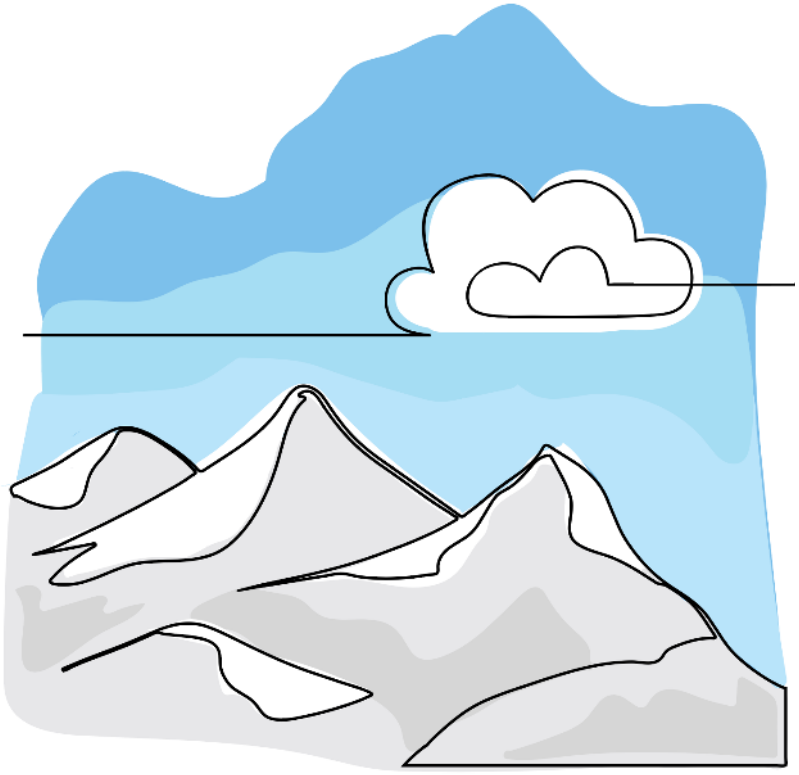


Climbing Mount Cloud

Manage your transition into the cloud.

What to expect and plan for as you make the transition to a scalable, function-rich, and compliant multi-cloud environment.

February 28, 2021

TEVORA™

The benefits of migrating your workload to the cloud are becoming hard to ignore.

Provable security, extended functionality, flexibility, scalability, and reduced costs are all compelling reasons to make this significant transition.

But the journey is not for the faint of heart. Maintaining the security, compliance, and functionality of your current operations while making the transition to a modern multi-cloud environment spread across multiple cloud service providers (CSPs) can be complex and demanding.

Climbing Mount Cloud

In many ways, your organization's transition to the cloud is like climbing a mountain. You'll face challenges along the way that push your team to its limits. To successfully summit Mount Cloud, you'll need the right tools and equipment. And don't forget to bring along an expert to guide you every step of the way.

TEVORA™

Overcoming Challenges

Mountain climbers must tackle challenges such as crevasses, blizzards, and avalanches. Organizations also face daunting challenges in migrating to the cloud. Here are some that our clients find to be the particularly difficult:

1. Defining infrastructure as code.

2. Layering in preventative controls.

3. Demonstrating compliance.

The good news is that there are excellent tools and resources available to help you overcome these challenges and realize the full benefits of a multi-cloud end-state

For example, “infrastructure as code” tools such as Terraform automate the process of configuring and deploying changes and upgrades to hundreds of cloud services, applications, and infrastructure components across multiple CSPs. They do this by enabling users to easily codify needed changes and upgrades in declarative config files that can be used to automate the configuration and deployment process. This approach can also be used to automate the process of demonstrating compliance with security standards.

Tevora has extensive experience working with clients to develop cookbooks and playbooks that leverage this infrastructure-as-code approach to enable automated, repeatable, and error-free deployments, which is an integral part of a leading-edge, multi-cloud environment. We’d welcome the opportunity to serve as your trusted guide to help you deploy these same tools and techniques.

TEVORA™

A Multi-Phased Climb

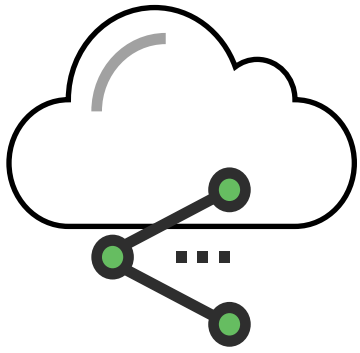
If you plan to climb Mount Everest, you need to break the journey down into multiple phases, with stops for rest and provisioning at base camps along the way. Your cloud migration should take a similar approach.

As much as you may want to complete your cloud transition in one giant step, the complexity and resource requirements of this significant effort make it more feasible to do it in multiple phases. In our experience working with clients, there are typically three phases of cloud evolution:

Phase 1 Legacy/Cloud Hybrid

Phase 2 Cloud-Native

Phase 3 Multi-Cloud



In this paper, we'll describe the characteristics of each phase from an infrastructure, security, network, and development perspective and address challenges companies face as they encounter each phase.

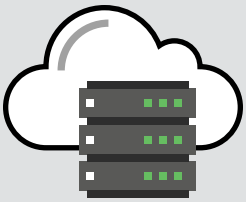
Our hope is that this information will help you plan for and execute the next steps in your journey to the cloud.

TEVORA

Phase 1 Legacy/Cloud Hybrid

In Phase 1, clients are just starting their climb into the cloud. They are shifting from being natively on-premise to a model in which some services are migrated to the cloud, and others remain in their legacy environment.

Infrastructure



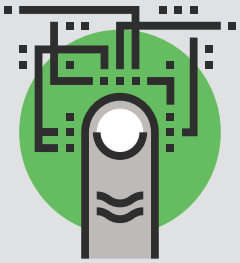
Clients are typically using a single CSP and still have one or more legacy on-premise data centers that they own and operate. Some core services continue to run on the legacy data center(s).

They are beginning the process of migrating services to the cloud using a manual provisioning process. Services are being augmented as they move to the cloud.

They are using a manual process to add cloud user accounts.

Legacy data center infrastructure can be scaled up or down to respond to changes in demand or business conditions. However, the tools to perform this are less automated than is the case with most cloud services. Users wishing to scale infrastructure up or down will submit a ticket to their IT organization to request the change.

Phase 1



Security and Compliance

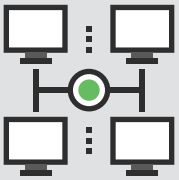
Security in the legacy environment is based on the assumption that applications will be running on in-house servers which can be fully controlled. Users generally access applications from within the company's trusted private network. The focus is on defending the perimeter of the network against attack. There is a high level of trust of applications, systems, and users that are inside the network perimeter.

As applications are migrated to the cloud, the focus of security begins to shift to authenticating and authorizing users, applications, and devices, using at least some Zero Trust approaches in which identity becomes the new perimeter. Many of these organizations are in the early stages of adopting Zero Trust capabilities.

Clients are beginning to shift some security roles and responsibilities to their CSP. For example, as they start to reduce reliance on firewalls, client staff may spend less time managing firewall rules. At the same time, responsibility for managing security of the hardware, software, and facilities infrastructure used to run cloud services is starting to shift to the CSP.

Demonstrating compliance with security standards such as FedRAMP, NIST 800-53, DFARS, HITRUST, and PCI-DSS is a manual and resource-intensive effort.

Phase 1



Network

Networking in legacy environments is host-based. Each application runs on a dedicated host within the company's private network. Each host has a dedicated IP address that identifies itself to the network. The network's primary job is to enable communication between hosts, applications, and users within the private network.

As applications are migrated to a CSP environment, networking focus begins to shift to a service orientation. Because services may be spread across multiple servers within their CSP environment, host-based networking is no longer a viable approach. This shift to service-based networking can be a significant change for many organizations.

Roles and responsibilities for network management are beginning to shift to the CSP as workload starts migrating to the cloud.

Development

Legacy environment developers create, test, and deploy applications on dedicated hosts within the company's network. Development and testing of cloud applications may be done on-premise or in the cloud.

TEVORA™

Phase 1

Challenges

1. Difficulty understanding what security controls are needed for cloud applications. Controls used for legacy applications are not effective for cloud applications.
2. Clients try to "lift and shift" existing legacy applications to the cloud but find that the resulting applications lack much of the fidelity that a native cloud application provides.
3. Legacy methods for enforcing change control are not effective in the cloud environment.
4. Clients struggle to securely deploy code to the cloud.
5. Performing incident response and forensic analysis when cloud environments are breached requires different tools, processes, and techniques.
6. Demonstrating compliance with security standards is a manual, resource-intensive effort.
7. Beginning to share security and network roles and responsibilities with a CSP can be tricky, and may result in things "falling between the cracks" if not managed carefully.

Solutions

1. Work with CSP to understand and document Phase 1 security and network roles and responsibilities to ensure nothing falls between the cracks.

2. Begin identifying, experimenting with, and selectively implementing:

   - Cloud-native applications, security controls, and change control solutions to replace legacy equivalents.
   - Infrastructure as code solutions for code deployment.
   - Automated breach detection and response solutions for cloud environment.
   - Automated compliance validation solutions for cloud environment.

TEVORA™

Phase 2 Cloud-Native

Many of the client's services have been migrated to the cloud using cloud-native applications and security controls. The client has a sizable footprint in the cloud, with many accounts. They are beginning to experiment with running workloads in more than one CSP environments (e.g., AWS and Azure).

Infrastructure

Most or all cloud applications have been migrated to a single CSP. Few, if any, applications remain in legacy data center(s).

The client is beginning to explore ways to move from a ticket-based approach for provisioning cloud applications, modules, and compute capacity to an automated, self-service, consumption-based model, where users can submit provisioning requests directly without having to submit a ticket to their IT organization. These automated approaches will often leverage "infrastructure as code" tools from companies like Terraform. Companies wishing to avoid vendor lock-in can use IaaS-agnostic tools, which are readily available, to automated these processes.

They are adding a large number of cloud user accounts manually and beginning to explore ways to automate this process.

Phase 2

Security and Compliance

The client has adopted an intermediate level of Zero Trust capabilities with identity-based security management to ensure that no user is implicitly trusted, even if they are accessing resources from within an internal network; all users requesting access to company resources are authenticated and authorized.

Moving to an identity-based security environment is a significant change for most organizations. It requires implementation of new tools and applications, which are available from companies like Okta and SailPoint.

Security considerations are built into automated provisioning processes to ensure a high level of security for cloud infrastructure, applications, and user accounts.

The client is beginning to adapt incident response and forensic analysis processes to the cloud environment.

Coordinating roles and responsibilities for security is becoming increasingly important as more and more cloud services are migrated to the cloud.

They are beginning to implement automated methods for demonstrating compliance with security standards such as FedRAMP, NIST 800-53, DFARS, HITRUST, and PCI-DSS.

Phase 2

Network

The client has fully transitioned to a service-based network for cloud applications and away from host-based networking, except for any remaining legacy applications running in on-premise data centers.

Development

Most, if not all, development and testing has moved away from the legacy environment and onto the cloud.

The client is beginning to explore tools to deploy infrastructure and applications within their cloud workloads. Securely deploying consistent cloud environments becomes increasingly important as the number of workloads scale.

TEVORA™

Phase 2

Challenges

1. Security teams are still manually reviewing most changes to production, which is time-consuming and error-prone. For example, we had one client that grew from 1 to 60 AWS accounts within a year, and the security team was manually approving each one. This was especially challenging because each account had its own unique environmental nuances. Not having common controls across their services meant that the client was spending most of their time fixing small items rather than focusing on more important security issues such as governance. These challenges can ultimately be addressed by developing private, self-service modules that can be consumed by the organization.

2. Performing incident response and forensic analysis in cloud environments continues to be difficult and is leading to exploration of new cloud-based approaches.

3. As security and network management roles and responsibilities are increasingly shared with the CSP, there can often be confusion about how these responsibilities are shared, which can lead to lapses in coverage.

4. Demonstrating compliance with security standards is still a manual, time-consuming, and resource-intensive effort and is becoming an increasingly significant problem as the number of cloud applications increases.

Solutions

1. Fully implement:

- Cloud-native applications, security controls, and change control solutions to replace legacy equivalents.
- Implement policy as code, to ensure secure and compliant deployments.
- Automated compliance validation solutions for cloud environment.
- Automated breach detection and response solutions for cloud environment.
- Infrastructure-as-code solutions for workload deployment, infrastructure changes, and user account additions and changes.

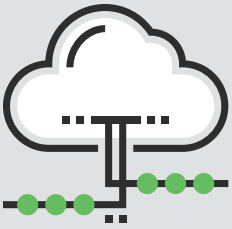
2. Work with CSP to understand and document Phase 2 security and network roles and responsibilities to ensure nothing falls between the cracks.

TEVORA™

Phase 3 Multi-Cloud

The client has migrated to a multi-cloud model, with cloud-native applications running on multiple cloud platforms (e.g., AWS, Azure, GPC).

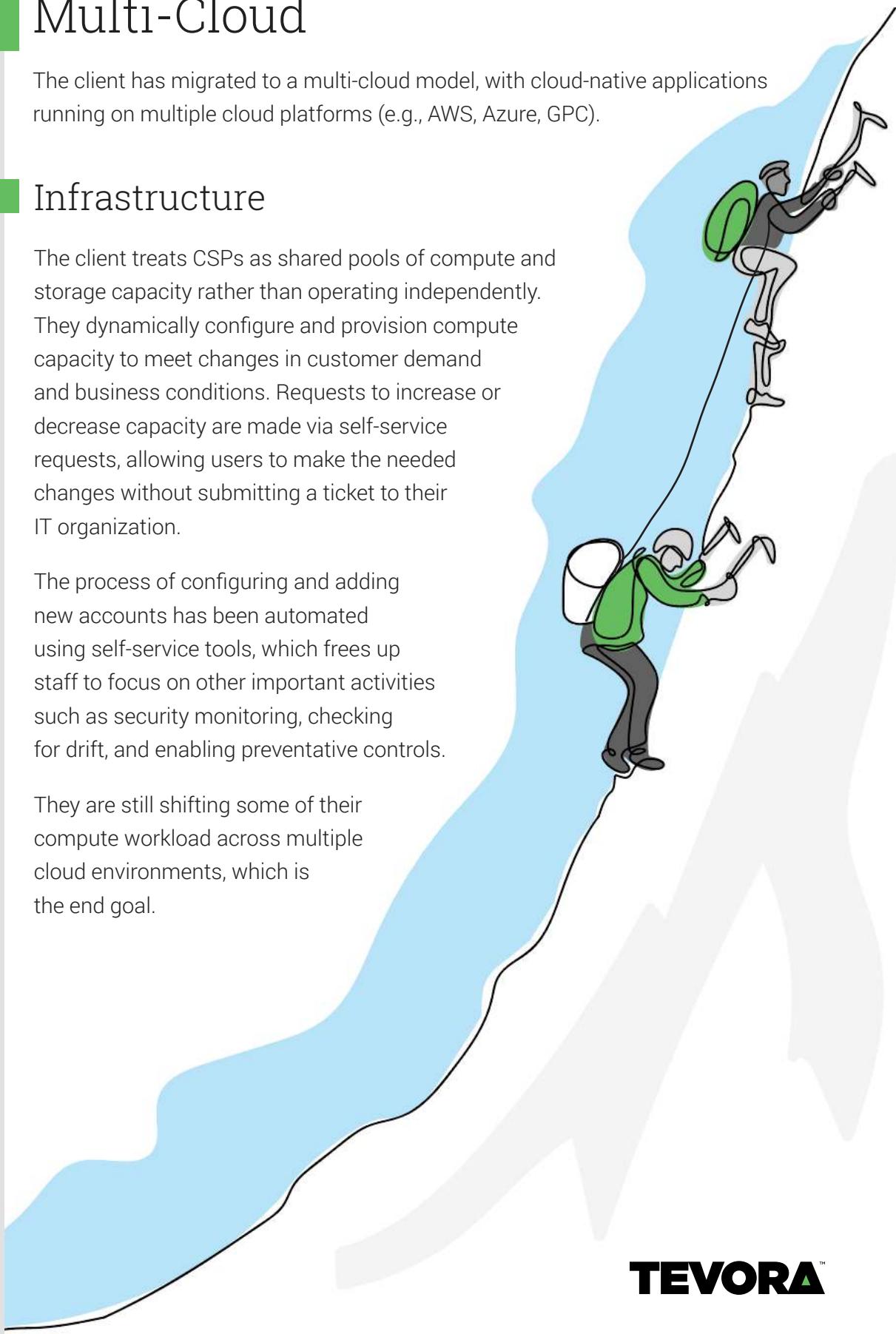
Infrastructure



The client treats CSPs as shared pools of compute and storage capacity rather than operating independently. They dynamically configure and provision compute capacity to meet changes in customer demand and business conditions. Requests to increase or decrease capacity are made via self-service requests, allowing users to make the needed changes without submitting a ticket to their IT organization.

The process of configuring and adding new accounts has been automated using self-service tools, which frees up staff to focus on other important activities such as security monitoring, checking for drift, and enabling preventative controls.

They are still shifting some of their compute workload across multiple cloud environments, which is the end goal.



TEVORA™

Phase 3

Security

The client is adopting advanced Zero Trust capabilities. They have integrated across cloud service provider environments, often federating accounts, as well as, using technologies such as Open Policy Agent (OPA) to unify policy enforcement across multi-cloud providers.

Accounts are added using a standardized “cookbook” approach that assures security and compliance requirements are automatically addressed for each user added.

They have begun to implement automated tools for demonstrating compliance with security standards.

Incident response and forensic analysis processes have been fully adapted for cloud.

Identical architectures are used in all CSP environments, enabling standardization of security controls and methods for performing audits.

Network

Service-based networking has been updated to enable communication between services across multiple CSPs.

Development

Most, if not all development and testing continues to be done in the cloud, and in some cases may occur in multiple CSP environments.

The client has implemented tools and capabilities to automatically deploy applications and application updates across a broad range of cloud environments.

TEVORA

Phase 3

Challenges

1. Client still distinguishes between cloud platforms (e.g., AWS, Azure, GCP) when spinning up services, which is time-consuming and error-prone.
2. Demonstrating compliance with security standards is still time-consuming and resource-intensive, which will continue to be the case until automated tools for doing this have been fully implemented.
3. Shared roles and responsibilities for security and network management must be coordinated across multiple CSPs.

Solutions

1. Implement a “single pane of glass” management tool that integrates information and processes across multiple cloud platforms, usually in the form of a unified console or dashboard. This saves time and reduces errors when spinning up services on multiple cloud platforms.
2. Review CSP shared responsibility model and plan to implement controls that fall under customer responsibility. Review CSP shared responsibility model semi-annually.
3. Complete implementation of automated compliance solutions across all cloud platforms.
4. Federate and leverage OPA to unify policy enforcement across CSP’s.

Summary

Here's a summary of the characteristics for each phase of cloud evolution.

Characteristics	Phase 1—Legacy/Cloud	Phase 2—Cloud-Native	Phase 3—Multi-Cloud
Infrastructure	• Single CSP • One or more legacy data centers running core services • Beginning to migrate services to cloud—manual provisioning process • Adding cloud user accounts manually • Ticket-based provisioning	• Single CSP; beginning to experiment with multi-cloud approach • Most or all cloud applications moved to cloud; few if any services remain in legacy data center(s) • Cloud services use cloud-native applications and security controls • Beginning to explore automated, self-service provisioning • Ramping up number of cloud user accounts added via manual process; beginning to explore ways to automate process	• Multiple CSPs running cloud-native applications and security controls • Dynamic provisioning of compute capacity and new accounts via self-service requests • Still some shifting of compute resources across multiple cloud environments
Security and Compliance	• Network is perimeter in legacy environment; high trust inside legacy data center(s) • Beginning to adopt Zero Trust in cloud environment where identity is perimeter • Responsibility for security of some infrastructure components beginning to shift to CSP • Demonstrating compliance with security standards is a manual and resource-intensive process	• Intermediate level of Zero Trust capabilities adopted; identity becoming new perimeter • All users requesting access to company resources are authenticated and authorized • Beginning to adapt incident response and forensic analysis processes to the cloud environment • Security is built into automated provisioning processes • Responsibility for security of most infrastructure components shifted to CSP • Beginning to explore automated methods for demonstrating compliance	• Adopting advanced Zero Trust capabilities • Security integrated across CSPs using technologies such as OPA to unify policy enforcement • Beginning to implement automated tools for demonstrating security standard compliance • Incident response and forensic analysis processes fully adapted for cloud • Responsibility for security of most infrastructure components shifted to multiple CSPs • Identical architectures used across CSP environments enabling standardization of security controls and audit methods
Network	• Host-based networking in legacy environment • Beginning shift to Service-based networking for cloud environment • Network management roles and responsibilities beginning to shift to CSP for cloud workload	• Networking for cloud environment is fully service-based • Host-based networking only used for any remaining legacy applications in on-premise data centers • Most network management responsibilities shifted to CSP	• Service-based networking updated to communicate across multiple CSPs • Most network management responsibilities shared across multiple CSPs
Development	• Development and testing of legacy applications done on legacy host(s) • Development and testing of cloud applications may be done on-premise or in the cloud	• Most, if not all, development and testing moved to cloud • Beginning to explore automated cloud application deployment	• Development and testing may be performed on multiple CSPs • Tools in place to automatically deploy cloud applications and updates

TEVORA™

We Can Help

If you have questions about this paper or would like Tevora to be your trusted advisor as you climb into the cloud, our team of cloud specialists can help. Just give us a call at (833) 292-1609 or email us at sales@tevora.com.

TEVORA™