ALERT LOGIC™

The Road to a Successful, Secure, and Stable Cloud Transformation

INTRODUCTION

Understanding Cloud Transformation

Many face a similar challenge: Create an agile organization that is able to adopt new technologies and processes to transform the business, while responding to market trends and staying competitive. Digital transformation and, by extension, cloud transformation, is the route that many choose. However, as with any major change program, there are inherent risks that must be avoided and challenges to overcome. Key among those is maintaining a secure posture. To achieve this, the role of security must be part of the foundation of your transformation strategy. Security can be an enabler to accelerate your organizational goals.

Cloud transformation is a journey in three parts:

1. **Migration**

   You'll define what migration means to your organization, establish your current state, and define your desired end-state and the positive benefits you'll unlock. You may be moving workloads and existing operations to the cloud, but rethinking how they should operate.

2. **Modernization**

   You'll embrace more efficient application delivery strategies and leverage modern technologies, such as container, serverless, or stateless architectures. You may be completely changing operating models or modernizing how you deliver your services.

3. **Optimization**

   You'll have the ability to operate at scale and may find it difficult to identify larger improvements. Optimization prepares you for the complexity of scale. It requires an organization to systematically discover multiple small changes across the organization that can yield the greatest overall rewards.

At the end of the journey, you will achieve many benefits:

- Opened new market and revenue opportunities
- Gained a competitive edge within your chosen market
- Improved customer satisfaction
- Improved the availability and performance of your applications
- Increased delivery and organizational agility

You achieve these benefits by precisely navigating through the three major parts of the journey and granting security a major place as an enabler along the way.

Preparing for Cloud Transformation

Cloud transformation preparation must begin with fully defining your desired end-state and obtaining agreement on transformation outcomes and benefits. Obtaining agreement includes internal alignment of stakeholders, which may require a culture change within the organization. Such a change is best brought about by articulating and educating the potential benefits at a customer, team, and individual level.

Stakeholders must include those accountable for customer needs, application and operational delivery, security teams, and any others that might be impacted. Cross-functional education should take place so that each stakeholder group understands what the others require and what benefits each will potentially attain to mitigate future conflicts.

As part of defining the end-state, ensure goals are manageable and can be met within the organization's framework, roles, and resources. Make sure each goal has a finite definition and isn't so nebulous that stakeholders can't fully understand it. Your goal definitions should be simple enough to reference throughout your transformation journey.

Any significant change contains risks, and cloud transformation is no exception. As part of preparing for the journey into the cloud, perform a complete risk assessment. For example, will this transformation disrupt business, for how long, and by how much? Will there be increased complexity that will have to be borne by stakeholders or customers?

This risk assessment includes security. Each phase of the transformation will have different security risks and requirements, and security must have a seat at the table right from the start.

Things to consider:

- *Clearly define desired outcomes*
- *Engage stakeholders early*
- *Establish manageable goals and measurable KPIs*
- *Perform a risk assessment*

Getting Started

Next, take the following steps:

1. Define the desired end-state for each phase of your cloud transformation, relating each to the customer, stakeholder, and organizational goals you have delineated.

2. Map each phase from starting state to end-state, including strategic and tactical steps within each framework.

3. Fully define and document the operational requirements of each phase:
   - Assess the skills and expertise required against your current organization
   - Evaluate the required processes and technology needed to deliver
   - Compare these to the detailed end-state to discover gaps

   Then, take any other necessary measures to get requirements fully defined.

4. Create or adopt key performance indicators (KPIs) for each phase to know whether your cloud transformation is succeeding and to what degree.

The above steps will lay a firm foundation for moving forward. You'll now be able to begin planning, budgeting, and assessing potential risks for the transformation. You can always refer back to these goals and requirements during any phase as the reasoning foundation for any decisions.

PHASE 1:

Cloud Migration

Cloud migration has a different definition for every organization, and you must define what it means to yours. This definition includes factors such as establishing your current state and defining your desired state, which contains positive benefits you will be able to unlock. It may include moving current workloads to the cloud and the lifting and shifting of existing operations while rethinking how they should operate.

In this phase, you are transforming the infrastructure cost model and operations to achieve a set of outcomes that enable the future phases. Fully explore and describe these outcomes for your organization that would include benefits such as expanding capabilities and expertise, the attainment of new markets, launching and offering new products, and changing how you service stakeholder's needs.

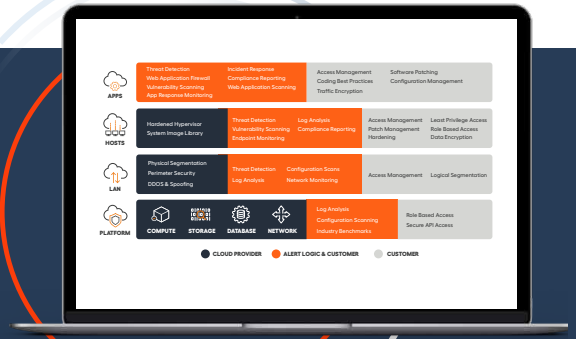
Outcomes should also include the improvement and the acceleration of time-to-value by eliminating security barriers. For example, in compliance-heavy industries such as healthcare or finance. This improvement should be a reduction from months to days or weeks.

Role of Security

Right from the beginning of migration, your organization must fully understand that security in the cloud is a shared responsibility. Fully separate your organization's security responsibilities and those of the cloud provider, for they are often different. Address and eliminate misconceptions about the cloud provider security provisions – they are not responsible for it all.

Overall, you and your teams should establish the security mindset for this migration. This means laying the security foundation for the desired state and should include a vision of greatly improved security post-migration.

If you need additional guidance on shared responsibility, be sure to leverage the guide on Defining a Shared Responsibility Model.



Best Practices

Here are a set of principles for your organization to follow throughout the migration phase:

- **Set objectives and KPI that are the size and scale of what you are aiming to achieve**. For example, an increase in scale to service customers, a decrease in costs, reduced operational overhead, or a reduction in needed, unforeseen changes.
- **Keep an eye on what is foundationally needed** to achieve long-term transformation goals, including factors such as automation and orchestration to recover from a breach.
- **Always research and assess the technologies** needed to realize outcomes and address risks you will need to remove as you proceed.

Don't Over-Reach!

You will not be able to solve everything for everyone. As long as the business and security issues are addressed, you should be able to continue moving forward

Real-World Example

Apervita, a rapidly growing healthcare cloud platform company, made sure that the objectives they set for cloud transformation could match desired outcomes. The nature of Apervita's offering as a compute platform required them to scale rapidly to accommodate minute-to-minute load changes. They found that the Amazon Web Services (AWS) offerings were well-suited to these dynamics.

This rapid scaling also meant the company needed a cybersecurity solution that would scale accordingly. The company faced a significant hurdle due to a scarcity of experienced cybersecurity professionals. Alert Logic was part of Apervita's solution to rapidly scale its security operations in a tight staffing market.

View Alert Logic Case Study

apervita

PHASE 2:

Cloud Modernization

At the outset of this phase, the decision needs to be made of what modernization will look like for your organization. If, for example, you are moving to a Software as a Service (SaaS) delivery model, there will be a major shift in responsibility as you are now responsible for customer data. You will likely need to embrace cost-effective application delivery modernization strategies, such as the utilization of container, serverless, or stateless architectures.

In this phase, you are transforming the business-impacting operations to achieve a set of outcomes that can dramatically improve revenue opportunities and cost savings. For modernization, these measurable outcomes could mean wholesale gains to your business, such as decreased cost, increased efficiency, and agility. You could unlock new markets, improve customer experience, and obtain new business.

The Role of Security

As your organization embraces new application delivery models, you should maintain consistent visibility and security of workloads so that the protection of environments and assets is maintained.

Here security must act as an enabler instead of a restrictive element. The right security processes and services will make it possible for you to meet your modernization goals rather than slow you down. For example, if you must comply with PCI DSS standards, make sure to utilize a security service that offers secure protection against loss of payment card data while allowing you to conduct business at today's rapid pace.

Maintaining a Security Mindset

As you modernize in the cloud, you and your teams need to accept that you will need to be tolerant of a level of risk you did not have before. You will need to ensure that your security processes match the velocity of change. The right security mindset enables the business to open uncharted opportunities, while keeping it safe.

Best Practices

As you proceed through Phase 2, bear these principles in mind:

- **Minimize and mitigate risks** and develop a sound knowledge of where risks lie. For example, container technology has great appeal for agility gains and cost benefits, but you will need to consider the visibility into containers.

- **Find the right velocity of change** that will not diminish your outcomes. If you move too fast, you may make mistakes that compromise your business through security risks.

- **Adopt the "buy-not-build" principle**, which states that where a function does not offer competitive differentiation and is not aligned with the business outcomes, examine the opportunity to leverage external services.

- **Manage new responsibilities.** Teams need to be well-aligned, with well-defined roles and responsibilities, along with clear goals that align with business goals.

- **Embrace technological advancements.** Consider services and systems that will address regulations in multiple markets.

Don't Repeat the Past

"Reuse and recycle" doesn't work in cloud modernization. Being wedded to a certain technology may have worked previously, but it now may prevent you from fully embracing opportunities and capabilities that could propel you into greater benefits.

Real-World Example

A good example of minimizing risk is considering the use of microservices.

Many applications use what is known as a monolithic model with a single-tiered software application with few components, all dependent on each other to function effectively. For example, you may have an e-commerce application with four main components: Product listing, shopping cart, reviews, and a payment system. All of these parts may be highly interdependent and would all access the same database. This model allows for each component to be a single point of failure. Additionally, suppose attackers breach any one component in the monolithic platform. In that case, the attacker can access all of the data or take the whole application offline.

With microservices, you could create a platform with four distinct microservice applications, each with its database and related services. Each application operates almost independently of each other. If one component happens to go down, the rest of the platform will still function and be secure.

PHASE 3:

Cloud Optimization

The optimization phase is largely driven by making multiple small changes across the organization that collectively yield the greatest overall rewards. In this phase, you are transforming the business' capabilities and opportunities by addressing inefficiencies in all areas to achieve a set of outcomes that can improve competitiveness and profit.

Optimization prepares you for the complexity of scale – it provides a cost-effective and scalable way for you to expand coverage. You will be able to transform inefficient processes and tools into dynamic solutions that address multiple essential requirements and integrate seamlessly into your operating model.

The Role of Security

There is another powerful outcome for this phase which applies to security: you do not have to compromise security for innovation. You can obtain enterprise-level security without the resource demand on your organization.

At this stage and beyond, the maintaining of security requires an understanding of business strategy. The security leaders – CISO or other roles – play a central part in this phase. The role of security leadership is changing; where before the CIO was the primary enabler of transformation, the CISO is now well placed to take on this role. In fact, enablement requires a team effort across C-suite and all leadership.

A Shift in the Perception of the Security Role

The role of security is no longer about "staying in their lane." The focus is more on business risk. It is about taking on an enterprise mindset – the good work the security professional is performing at an operational level should be positioned with the controls they are putting in place and tied to the benefits yielded as a result. These benefits should be viewed as to how they are helping mitigate bigger picture risks – for example, not being competitive in the market.

Best Practices

Here are principles to keep front-of-mind while proceeding through the optimization phase:

- **Fully assess requirements against changes** that can deliver optimization. Understand which functions to target for improvement over time, such as application and security monitoring. Identify functions that involve the most manual or time-costly activities.
- **Align security transformation with cloud transformation** by seeking out opportunities to optimize security parallel to cloud transformation.
- **Fuel growth through continuous improvement** and marginal gains. Adopt advanced techniques founded on the basics of automation and code.
- **Create experts within the organization** who understand business goals and business value, and how to architect solutions to unlock your performance and discover better ways to solve challenges.
- **Make more efficient use of resources**, outsourcing where needed. Where it makes sense, shift from DIY to managed services – a prime example being security – to perform some of that heavy lifting.

ALERT LOGIC™

Eliminate Undifferentiated Heavy Lifting

Werner Vogels, chief technology officer of Amazon.com, coined the term "undifferentiated heavy lifting" several years ago to describe all the hard IT work that companies do that does not add value to the mission of the organization.

Real-World Example

A good example of minimizing risk is considering the use of PCI Pal is a provider of PCI DSS (Payment Card Data Security Standard) compliant solutions for contact centers taking Cardholder Not Present (CNP) payments.

Since its initial cloud launch in 2016, PCI Pal today has instances in the US, Canada, Germany, and Australia. The company attributes their deployment speed and their ability to handle large scale telephony traffic to re-engineering their telephony offering utilizing the AWS environment.

While optimizing their cloud environment, PCI Pal realized they did not have the workforce to handle the heavy lifting of a public cloud security model. They successfully outsourced to an expert third-party partner – Alert Logic – and proceeded through with a very successful cloud optimization. Today, the company utilizes Alert Logic's fully managed and continuous threat detection and response offering, which provides the security the company requires for their rigorous cloud operation.

View Alert Logic Case Study

pcipal®

Conclusion

Let's summarize the three phases and reiterate the best practices and principles for each major phase of your transformation.

Phase 1: Cloud Migration

You will define what migration means to your organization, establish your current state, and define your desired end-state and the positive benefits you will unlock. You may be moving workloads and existing operations to the cloud, but rethinking how they should operate.

- **Set objectives that are the size and scale of what you are aiming to achieve** (for example, an increase in scale to service customers).
- **Keep an eye on what is foundationally needed** to achieve long-term transformation goals.
- **Always research and assess the technologies** needed to realize outcomes and address risks you will need to remove as you proceed.

Phase 2: Cloud Modernization

You will embrace more efficient application delivery strategies and leverage modern technologies, such as container, serverless, or stateless architectures. You may be completely changing operating models or modernizing how you deliver your services.

- **Minimize and mitigate risks** and develop a sound knowledge of where risks lie, such as visibility into containers.
- **Find the right velocity of change** that will not diminish your outcomes.
- **Adopt the *buy-not-build* principle** by examining the opportunity to leverage external services.
- **Manage new responsibilities.** Teams need to be well-aligned across roles, responsibilities, and business goals.
- **Embrace technological advancements** like services and systems that address regulations in multiple markets.

Phase 3: Cloud Optimization

You will have the ability to operate at scale and may find it difficult to identify larger improvements. Optimization prepares you for the complexity of scale. It requires an organization to systematically discover multiple small changes across the organization that can yield the greatest overall rewards.

- **Fully assess requirements against changes** that can deliver optimization.
- **Align security transformation with cloud transformation** by seeking out opportunities to optimize security parallel to cloud transformation.
- **Fuel growth through continuous improvement** and marginal gains, such adopting advanced techniques.
- **Create experts within the company** who understand business goals and business value.
- **Make more efficient use of resources** by outsourcing where needed, like managed services for security.

Alert Logic is ready to fully enable your cloud transformation.

Contact one of our cloud security experts today.

ALERT LOGIC™