ARMOR

ASSESS & PLAN
VALIDATE
BUILD
MIGRATE
OPTIMIZE

WHITE PAPER

THE SECURE CLOUD MIGRATION FRAMEWORK

A HOW-TO GUIDE

TABLE OF CONTENTS

About the Secure Cloud Migration Framework 03

Envision Security and Compliance Transformation with Your Cloud Migration 04

11 Strategic Considerations Before Starting Any Migration Project 07

Starting Your Secure Cloud Migration 16

The Secure Cloud Migration Framework 18

- Assess & Plan 19
- Validate 27
- Build 30
- Migrate 36
- Optimize 40

ABOUT THE SECURE CLOUD MIGRATION FRAMEWORK

In the future, all digital innovation will be in the cloud. And as infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) capabilities continue to evolve and be adopted, everything you do will essentially become a "workload." However, first you've got to get to the cloud as smoothly as possible with security and compliance controls designed from the outset.

The Secure Cloud Migration Framework is designed to help you address all of the common elements involved in the overall migration of your applications and data to the cloud with a strong security and compliance overlay. This helps you protect them while meeting compliance with major frameworks such as PCI DSS, HIPAA/HITRUST, GDPR and others.

This framework is also designed to offer an attainable vision for security and compliance in the cloud that elevates your security posture while enabling continuous compliance across your cloud footprint.

ENVISION SECURITY AND COMPLIANCE TRANSFORMATION WITH YOUR CLOUD MIGRATION

There is a very real opportunity to redefine how security and compliance for your workloads are done in the future. You can implement a multi-layer, defense-in-depth security and compliance posture that is continuously evaluating adherence to a global security policy while protecting your sensitive applications and data in the cloud. And you can address both "Accidental" cyber risk—the risk introduced from things such as cloud misconfigurations and open settings—and "Intentional" cyber risk—risk caused by bad actors targeting your cloud workloads and data.

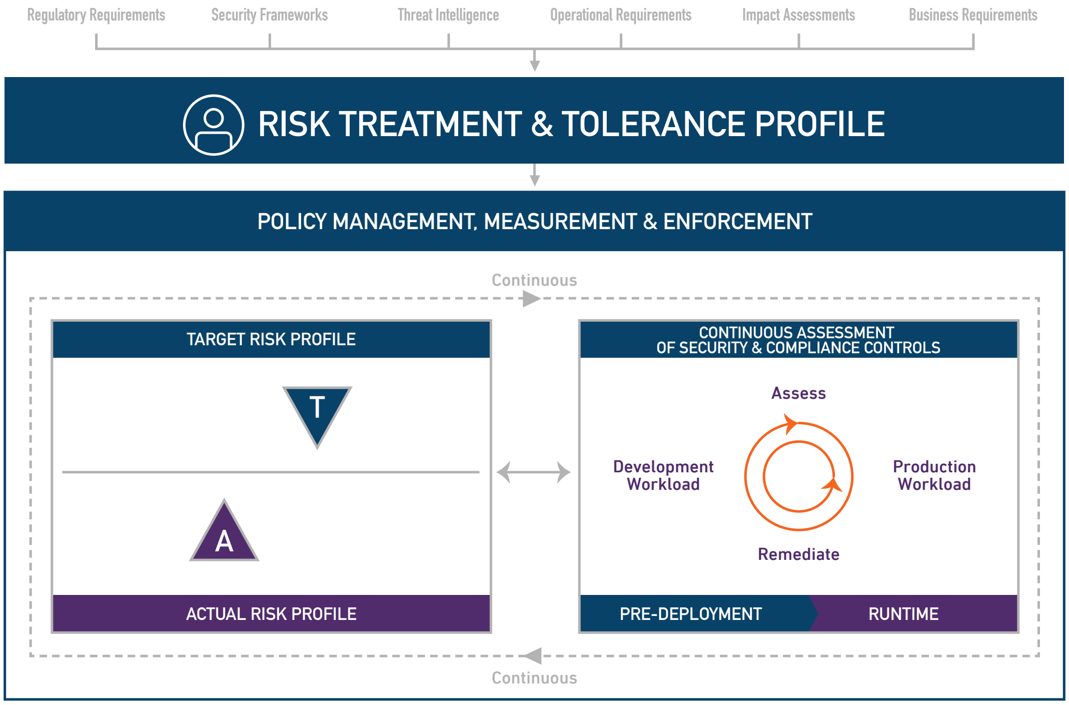
The cloud represents a fundamentally different way of computing and, as a result, offers and even requires a fundamentally different way of securing applications and data or addressing adherence with compliance frameworks. The graphic below provides perspective on some of these differences.

TRADITIONAL SECURE COMPUTING MODEL	SECURE CLOUD COMPUTING MODEL
Inefficient Usage & Billing Models	Utility-based Billing
Turn-up in hours and minutes	Turn-up in minutes and seconds
Infrastructure Intensive	Infrastructure-less
Capex/Opex Blended	Opex
Highly Manual	Highly Automated
Inefficient Usage & Billing Models	Utility-based Billing
Centralized Security Function	Democratized Security Function
On-Premise Security Expertise	Cloud Security Expertise
TCO for Infrastructure	TCO for Security
Siloed Visibility	Unified Visibility Across Environments
Compliance Management	Continuous Compliance

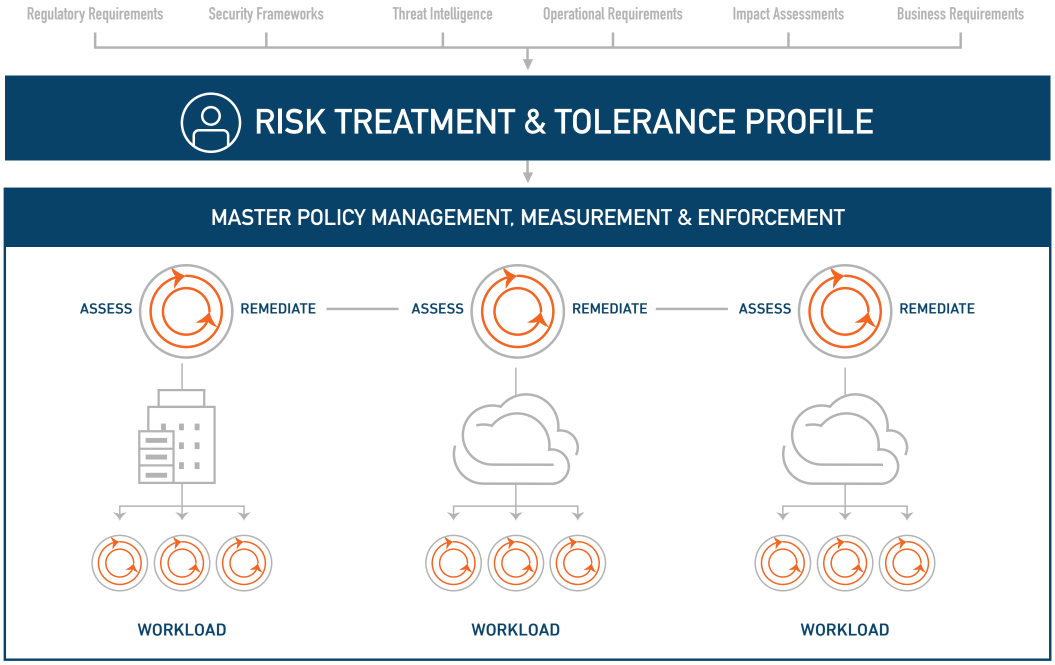
The fact is that new capabilities such as Cloud Security Posture Management (CSPM) combined with Cloud Workload Protection (CWP) allow you to entirely reconsider security operations around your deployments in the cloud. Because the topic is lengthy in and of itself and not the purpose of this paper overall, we won't go into detail. However, the charts shown provide a good representation of the power of tools such as CSPM and CWP integrated with cloud native capabilities.

We're talking about creating an automated and continuous security and compliance function that monitors adherence of security and compliance controls to a larger, global security policy. This monitoring assesses, reports on, and even automatically remediates "drift" away from that global security policy.

Here is the concept applied for a single instance or workload in the cloud:



Now, think about that same process being applied across tens, hundreds, and even thousands of cloud-based workloads, and the resultant scale benefits in doing so:



This is huge. Managing cyber risk through one global security policy means tremendous efficiencies for security, compliance, and secure application development efforts while completely changing the cyber risk equation for businesses. And imagine that this management system also acts as an automated mechanism to provide guide rails for DevOps and Development teams who may be deploying applications into the cloud. Because the tools are largely automated and can easily inject into the early DevOps cycle—"security as code"—developers are able to seamlessly adhere to policy controls without impacting their ability to produce new code.

THE BOTTOM LINE

With the opportunity to reimagine and implement a security and compliance governance approach like that discussed above, it behooves IT and IT Security teams to seriously consider this as well as other approaches to security and compliance adherence when deploying applications to the cloud.

11 STRATEGIC CONSIDERATIONS BEFORE STARTING ANY MIGRATION PROJECT

Before you embark on your cloud migration project and overall journey to the cloud, it's critical to understand and consider a number of strategic areas first. These areas should influence your organization's thinking and planning regarding what drives your organization to the cloud and how you secure the applications and data that reside there.

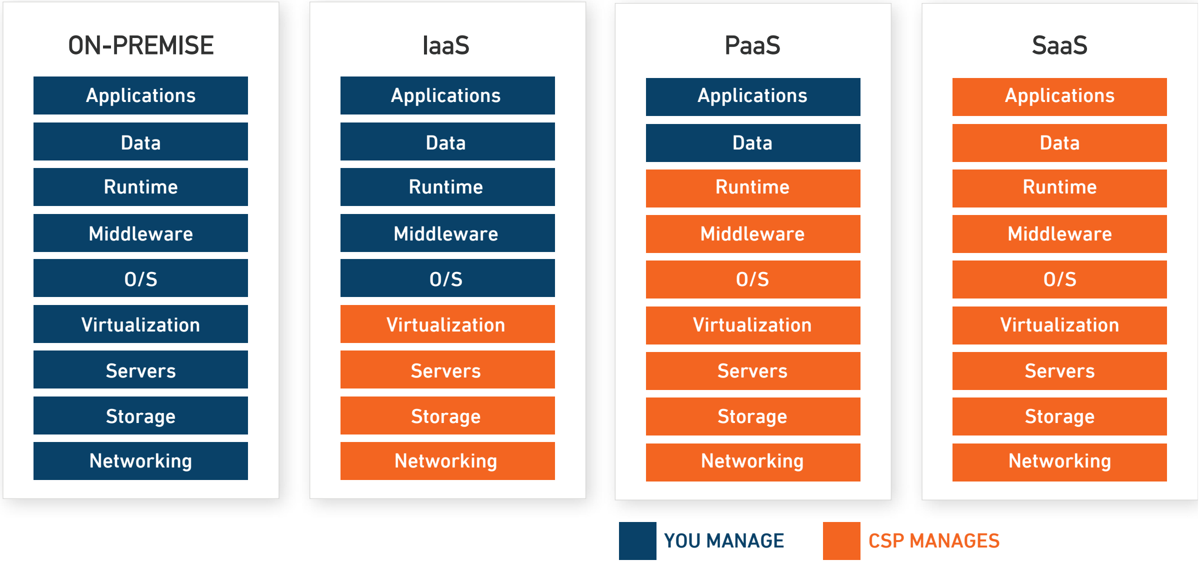
There is no order to the areas identified here as each may hold different weight based on the particular plans and needs of each organization.

1. SHARED RESPONSIBILITY

In the cloud, Shared Responsibility is black and white. The various cloud service providers go out of their way to make it clear where their responsiblilty ends and yours begins.

Before embarking on your cloud migration journey, make sure you know exactly what your organization is on the hook for across private cloud, IaaS, PaaS and SaaS cloud computing models.

Shared Responsibility is a key tenet for any cloud or hosted solution. And the level of responsibility the customer owns varies based on the different cloud platform types as depicted here. IT, Security, and DevOps teams need to have a keen understanding of shared responsibility for each cloud or hosted solution employed.



ON-PREMISE	IaaS	PaaS	SaaS
🟦 Applications	🟦 Applications	🟦 Applications	🟧 Applications
🟦 Data	🟦 Data	🟦 Data	🟧 Data
🟦 Runtime	🟦 Runtime	🟧 Runtime	🟧 Runtime
🟦 Middleware	🟦 Middleware	🟧 Middleware	🟧 Middleware
🟦 O/S	🟦 O/S	🟧 O/S	🟧 O/S
🟦 Virtualization	🟧 Virtualization	🟧 Virtualization	🟧 Virtualization
🟦 Servers	🟧 Servers	🟧 Servers	🟧 Servers
🟦 Storage	🟧 Storage	🟧 Storage	🟧 Storage
🟦 Networking	🟧 Networking	🟧 Networking	🟧 Networking

🟦 YOU MANAGE 🟧 CSP MANAGES

2. DEFINE YOUR MIGRATION GOALS

Are you looking to achieve great speed in your IT operations? Do you want to be able to respond more nimbly to changes in technological capabilities? Is your main goal improving the customer experience—or enhancing internal efficiencies?

Understanding what you want out of your cloud migration is the first step toward realizing it.

There are many great resources you can use to articulate and justify why your organization should migrate applications to the cloud. However, "getting to the cloud" isn't the overall objective. Instead, there are usually key business and technical drivers powering consideration of the cloud as an enabler. And we'd make the argument that achieving rapid digital innovation in the future will rely on the cloud as the all-important enabling platform.

3. TRANSITIONING TO A SOFWARE-DEFINED SECURITY MODEL

Migrating applications to the cloud represents a fundamental shift in how security and compliance are done versus in the past. We're talking about moving to a model where everything is software-based. There is no hardware, and security is no longer defined by the perimeter.

The cloud represents an entirely different security and compliance paradigm. The faster Security and DevOps teams go from a focus on traditional on-premise and appliance-driven security and compliance practices to incorporate new skill sets and experience in securing cloud-based workloads, the better positioned they will be to help the organization accelerate the pace of innovation securely.

Security and DevOps teams need to honestly evaluate their cloud expertise, put plans in place to address gaps, and develop a solid cloud security competency across their staff. In fact, enterprises are already making this shift with 66% reporting they already have a central cloud team in place, according to the RightScale 2019 State of the Cloud Report™. That figure drops substantially to 31% of SMBs having a central cloud team in place.

4. VENDOR LOCK-IN

Whether it's a standard policy not to be over-reliant on one vendor, or a corporate directive on high, you will need to consider the extent to which you are comfortable with using a single public cloud provider platform and how much you are willing to lock in your investment in that one platform.

With constant concerns for disruptors entering the marketplace, many organizations may employ a cloud-agnostic strategy to prevent enabling a potential competitor. Others may see a cloud-agnostic approach simply as an effective risk mitigation strategy. Identify whether your organization is likely to have concerns for over-investment in a single cloud platform and, if so, plan accordingly to address it.

5. MULTI-CLOUD IS BOTH A STRATEGY AND A NATURAL OUTCOME

Like a cloud-agnostic policy, pursuing a multi-cloud strategy can come as a choice by leadership or as a natural result of the analysis to determine what cloud environment best suits the specific requirements for each of the applications you are looking to deploy.

Whether it's a cloud-agnostic policy driving adoption or the findings of analysis that determine different applications have individual requirements best suited by different platforms, you may find your organization on the path to a multi-cloud strategy or policy. We argue that this outcome is inevitable for most organizations. Get ahead of whether your organization will pursue a multi-cloud approach and even outline what your organization's approach is now and potentially in the future.

6. ACCIDENTAL AND INTENTIONAL

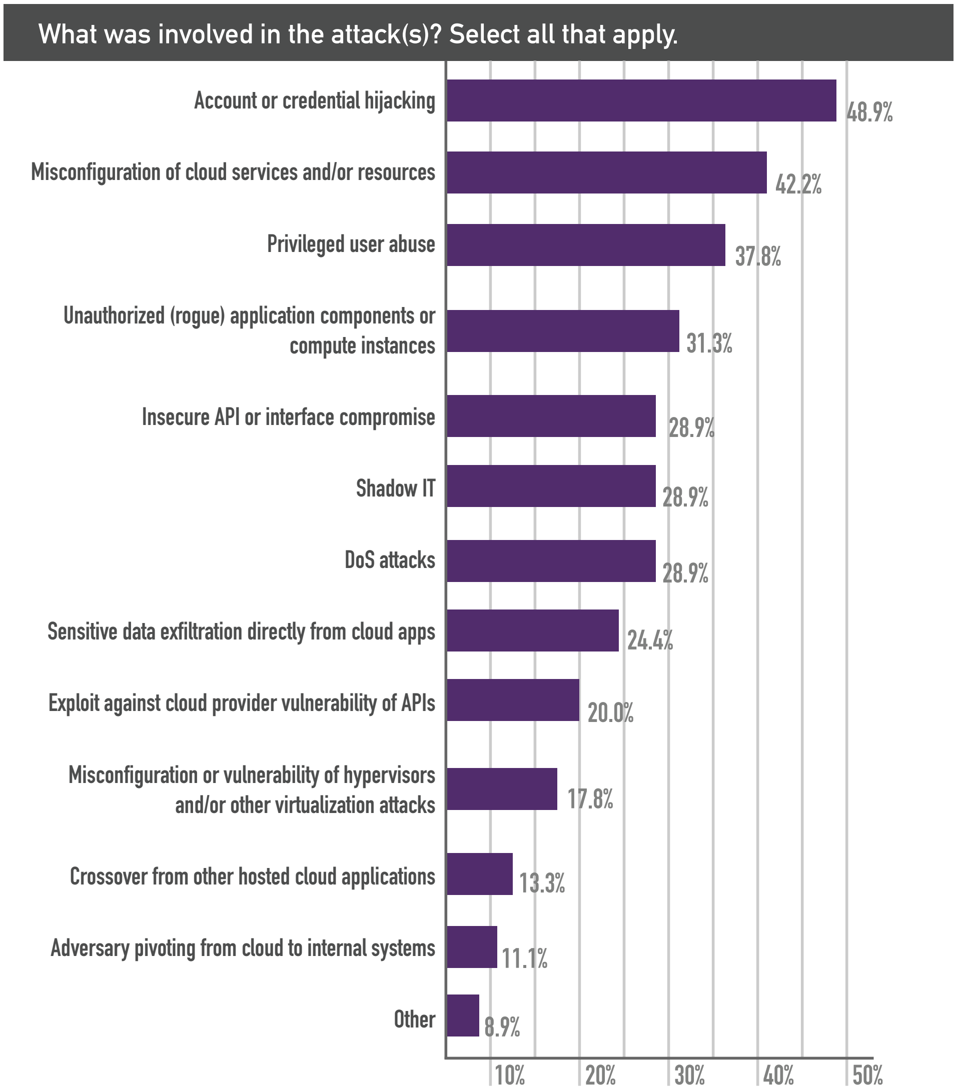
Because of the lower level of familiarity and experience with public cloud platforms, it's best to think of the cyber risk your organization can be exposed to. It could be "Accidental" cyber risk, or the risk introduced by misconfigurations, improper settings, and the honest mistakes (and not so honest) that can expose applications and data in the cloud. It could also be "Intentional" cyber risk, the risk introduced by threat actors targeting your application and data.

As organizations increasingly embrace the cloud, they must address both “accidental” and “intentional” cyber risk as part of their shared responsibility for security in the cloud. Cyber risk can be simplified down to the accidental risk introduced from things such as cloud misconfigurations and open settings and what IT or developers might do, to the intentional risk caused by bad actors targeting your company or ransomware encrypting your data.

Fortunately, emerging technologies and capabilities such as Cloud Security Posture Management (CSPM) and Cloud Workload Protection (CWP) provide innovative approaches to address both areas of cyber risk while automating security and compliance processes.

Cloud Workload Protection provides multi-layer defense-in-depth protection for your workloads from intentional threats, helping you meet the requirements of your portion of the Shared Responsibility model. Typical solutions integrate host-based IDS (HIDS), Malware Protection, File Integrity Monitoring, and Vulnerability Scanning and may include expert monitoring 24/7/365 as well as some degree of integrated incident response. These solutions can also be deployed across cloud, on-premise, and hybrid environments for unified visibility.

TYPES OF INTENTIONAL ATTACK THREAT VECTORS



SANS 2019 Cloud Security Survey - 2019

Cloud Security Posture Management technologies help you continuously discover, assess, and remediate security and compliance controls across your environment in the cloud. This includes identification of cloud misconfigurations and improper settings as a result of honest mistakes and negligence that could put your applications and data at risk of exposure. In addition, CSPM solutions can provide an opportunity for organizations to establish a global security policy for assessing and managing risk across their cloud environments.

The combination of the two solutions, in concert with other security protections, represents a powerful opportunity to elevate the security and compliance posture for your cloud environment.

7. REACTIVE VS. PROACTIVE

Traditional security operations in the on-premise world are largely reactive in nature, reacting to the first sign of a threat hitting the perimeter or the first missed checkbox on a compliance audit. The cloud changes everything.

With new capabilities such as Cloud Security Posture Management (CSPM), Cloud Workload Protection (CWP), and native tools being rolled out regularly, IT, Security and DevOps teams can put security on a proactive footing while automating and simplifying operations in the process.

It's important to recognize this opportunity to drive a stronger security posture while capturing efficiencies at the same time. Make sure you engage your IT, Security, and DevOps teams responsible for application and data security on this and other topics in this paper—thus providing time to consider and capitalize on the opportunities the cloud presents in redefining the active nature of your security and compliance operations.

ACCIDENTAL CYBER RISK

Over a 2-year period, 920 million records were inadvertently exposed publicly as a result of an AWS S3 misconfiguration. Of the 13 incidents identified, 8 involved data exposed by an affiliate, partner, or customer of a larger organization.

— Armor Research

8. SECURITY EARLIER IN THE DEVOPS CYCLE

DevOps practitioners must be able to drive secure code development and deployment with as little friction and complexity as possible along the way. And anything that gets in the way of delivering more code in support of business objectives typically means serious trade-offs.

However, security and compliance practices integrated early into the DevOps cycle and automated to enhance the overall protections afforded to your applications is entirely possible in the cloud.

Pressure to accelerate the pace of business puts demands on the teams involved in supporting business initiatives and innovation. That places pressure on Development and IT teams responsible for pushing out new code and supporting those initiatives and innovation. Security and compliance functions must line up to the new reality that controls are deployable at the speed of development with as little friction as possible.

By integrating security and compliance controls early into the DevOps process, IT, Security, and DevOps teams can match the pace of development. In addition, new capabilities can act as guide rails for best security and compliance practices for developers through their coding efforts.

Last, this approach begins to put the goal of immutability within reach.

9. IMMUTABILITY

Imagine the future where security protections are enhanced by a constant ebb and flow of your instances being wiped and recreated daily or even hourly. This makes it even harder for an advanced threat actor to establish a foothold in your environment and have the time to cause any actual harm.

IT, Security, and DevOps teams need to be thinking now about the pieces they can put in place to move toward immutable infrastructure and workloads. As cloud security experts, we see a lot of promise in adopting this kind of regimen. Security and compliance protections are integrated early into the DevOps cycle, and workloads are unchangeable once they are put in production—thus increasing the difficulty for threat actors to gain and maintain a foothold in your cloud environment.

Additional benefits of immutability include:

- Eliminates disruption to product applications for patching and updates as these are done on the gold image and then rolled out.
- Reduces risk of disruption or downtime associated with testing as testing is performed on the gold image.
- Accelerates roll-out of application updates.
- Easily detects unauthorized changes to production applications (combined with security capabilities such as File Integrity Monitoring), resulting in automated deletion and regeneration of the application.

As organizations consider the advantages of immutable infrastructure, they should be considering the business and technical advantages of containers as one aspect of this infrastructure.

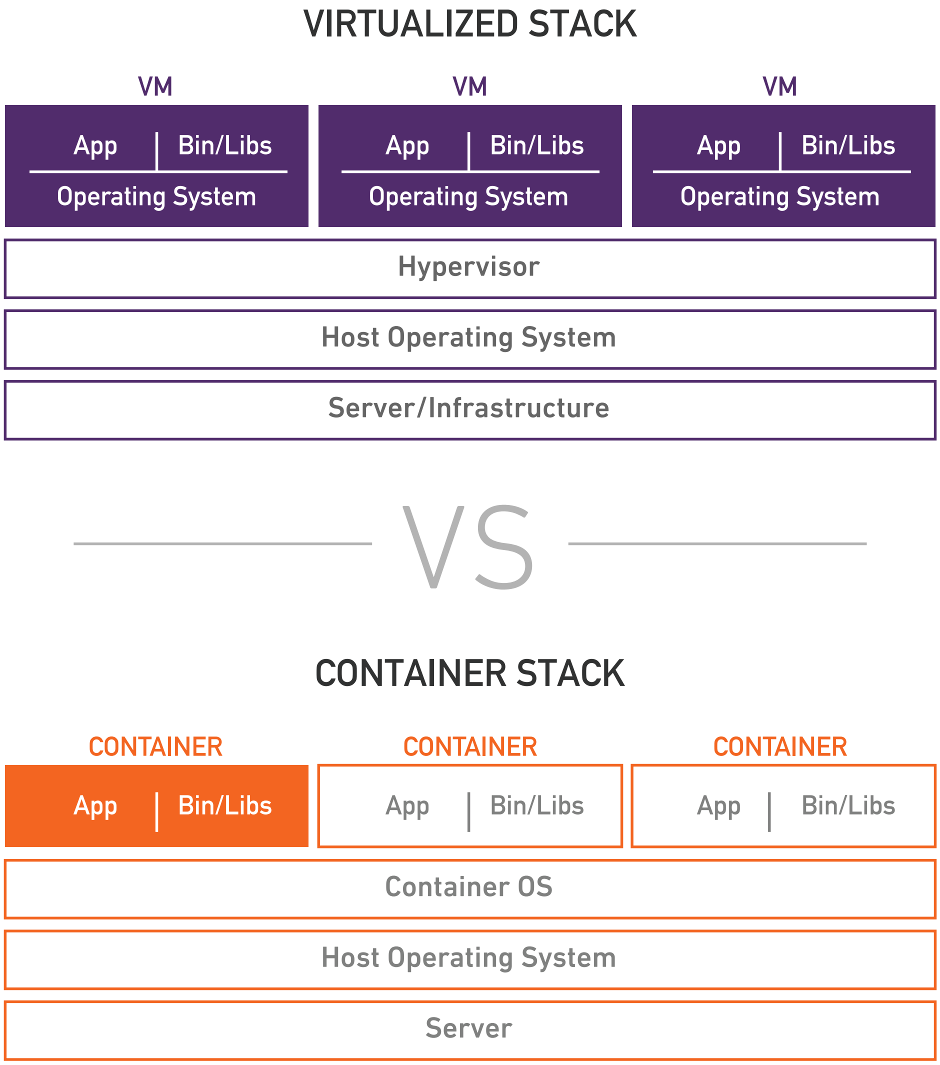
10. ANTICIPATING OPPORTUNITY

Containers, Serverless, and Microservices architecture present tremendous benefits for organizations—ease of deployment, portability, scalability, and the ability to act as a hedge against vendor lock-in.

As you plan your migration, you will want to future-proof your planning to provide allowances for container usage and serverless deployments, as well as identify any applications where a microservices architecture will make sense (not for every organization or for just any application).

Containers are as they sound—they hold something. In this context, a container is a logical storage box that houses an application and its related components. The concept of containers is not new, though their usage has accelerated with the increased adoption of the cloud. Docker, a computer program that "virtualizes" (i.e., containerizes) operating systems (OS), refers to containers as simply, "a standardized unit of software." Forrester offers a more specific description: "Containers bundle applications with the software libraries that they depend on, allowing developers to create 'build once, run anywhere' code making applications very portable."

DevOps and development teams are the primary force driving the adoption of containers because of the accelerated time-to-market for deployment of testing and production environments for new applications. Meanwhile, IT may be pushing the use of containers to move legacy applications into the cloud with the intent to refactor some of those applications in the future.



Though security teams may see the advantages inherent in the use of containers, it's unlikely they would push container usage unilaterally—especially without clear security solutions in place to protect them. But development and DevOps already see the value of containers and leverage them. Smart security teams would likely want to exploit their full security value in the future.

- PRODUCTION DEPLOYMENTS – According to 451 Research, 52% of enterprises are either in the initial stages or have broadly deployed production applications in containers.
- MICROSERVICES DEPLOYMENT – Containers are particularly ideal for microservices deployments, which break down traditionally monolithic or large-scale application architectures into specialized micro applications.
- DEPLOYMENT OF DEV APPLICATIONS FOR TESTING – Containers allow for rapid deployment of applications under development and testing, eliminating the complications associated with configuring and managing the underlying host OS. The ability to spin containers up and down quickly and easily aligns with the needs of DevOps and developer teams.
- "LIFT AND SHIFT" OF LEGACY APPLICATIONS – Whether refactored or not, deploying legacy applications in containers can accelerate the shift to the cloud, while freeing up an enterprise's costly on-premise resources and footprint.
- RUNNING OF TRIALS AND PILOT PROJECTS – Containers also provide an efficient mechanism to run trials and pilot projects without the additional overhead associated with managing the OS or infrastructure.

For more information on the value of containers, see our white paper, "RISK CONTAINED. DEVELOPMENT UNRESTRAINED."

11. THE SOFTWARE-DEFINED NETWORK

Be sure to research and comprehend how a Software-Defined Network model based on Zero Trust and the use of microsegmentation could enhance security across your presence in the cloud. Whether this is something your organization is ready for or not, be cognizant of how your organization could adopt such a model in the future.

STARTING YOUR SECURE CLOUD MIGRATION

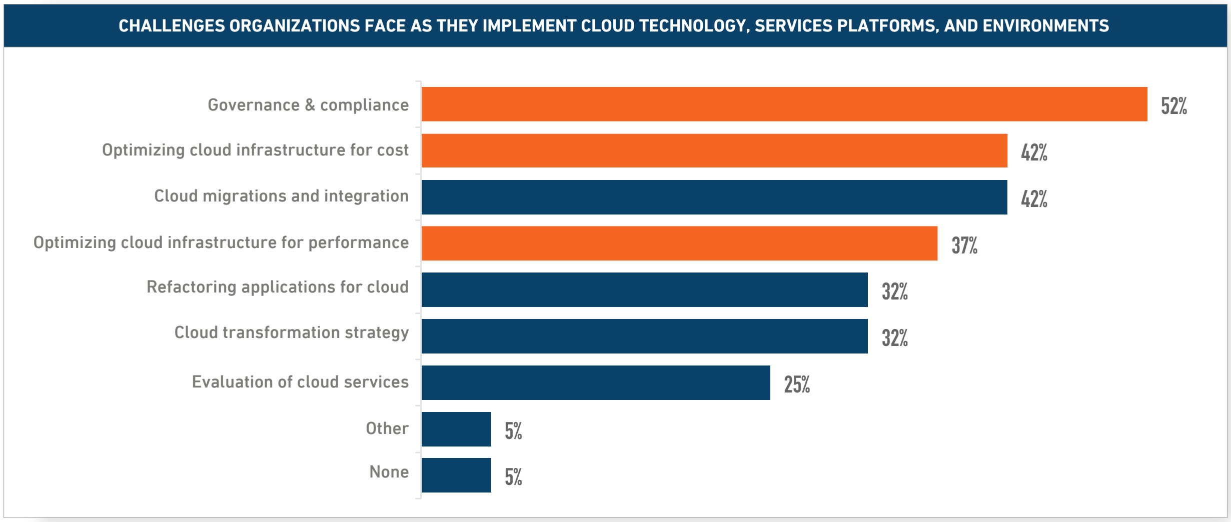
NOW THAT YOU ARE READY TO JUMP INTO YOUR ACTUAL CLOUD MIGRATION JOURNEY, THERE ARE A FEW ADDITIONAL PERSPECTIVES FOR YOU TO CONSIDER.

RISK MANAGEMENT, NOT JUST PROJECT MANAGEMENT

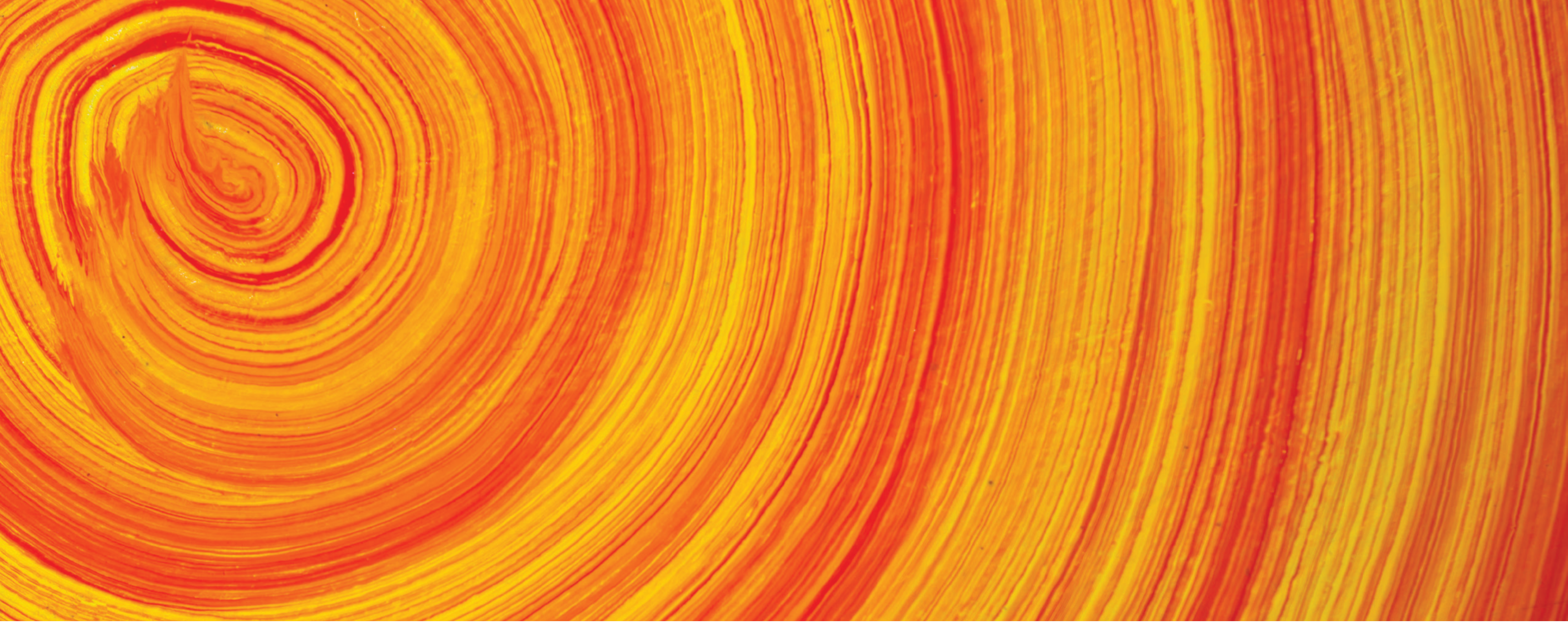
The cloud migration process is both a project management process and a risk management process. From a risk management standpoint, the process is intended to minimize the risk to investing in migrating applications to the cloud. The first stages—Assess and Plan, and Validate—represent the information-gathering and planning phases that will determine how the rest of the project will go. View the process through a risk management lens, and it's likely your results in the early stages will yield the results you are looking for in the latter stages.

LEARN FROM THOSE WHO HAVE GONE BEFORE YOU

Learn from those who have gone before you as you aren't the first to migrate applications to the cloud, and you won't be the last. We included this chart to remind you of the importance of proper due diligence and planning in your cloud migration process. As you can see, security/governance/compliance concerns still hold the No. 1 spot in terms of challenges. The next three highest values all represent challenges associated with cloud migration and optimization.


CHALLENGES ORGANIZATIONS FACE AS THEY IMPLEMENT CLOUD TECHNOLOGY, SERVICES PLATFORMS, AND ENVIRONMENTS

Source: 451 Research

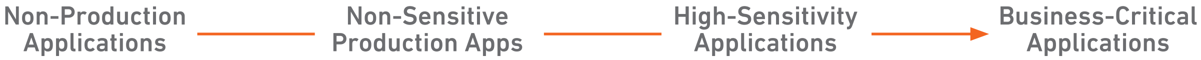


SHARED RESPONSIBILITY MODEL

As we mentioned before, the Shared Responsibility Model represents a perfect starting point for understanding each cloud provider's security capabilities, and ultimately, what your organization will need to supplement. Be intimately familiar with the Shared Responsibility Model for each cloud platform your organization opts to utilize.

START SMALL

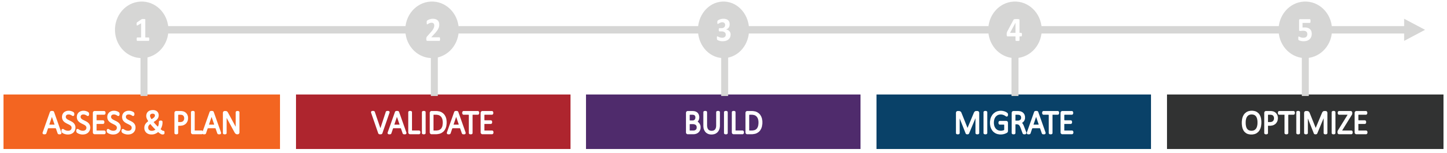
Consider starting your cloud migration journey with smaller-scale, less sensitive applications to prove out processes and build experience across your team. These may even be non-production applications. As you go about your first migrations, keep an eye out for learnings and best practices that apply to your more sensitive applications to migrate. What defines the "sensitivity" of applications may be driven by whether the application (and related data) is subject to a compliance mandate, the application has a direct revenue impact, etc. The simple graphic below represents this continuum:



Non-Production Applications — Non-Sensitive Production Apps — High-Sensitivity Applications → Business-Critical Applications

THE DEVOPS CYCLE

Think about how to integrate security and compliance capabilities further left into the DevOps cycle. The nature of the cloud means that organizations have an opportunity to fundamentally change how security against threats is done in the future, and that means things such as earlier integration into the DevOps cycle, immutability, and automated application replenishments.



1 ASSESS & PLAN

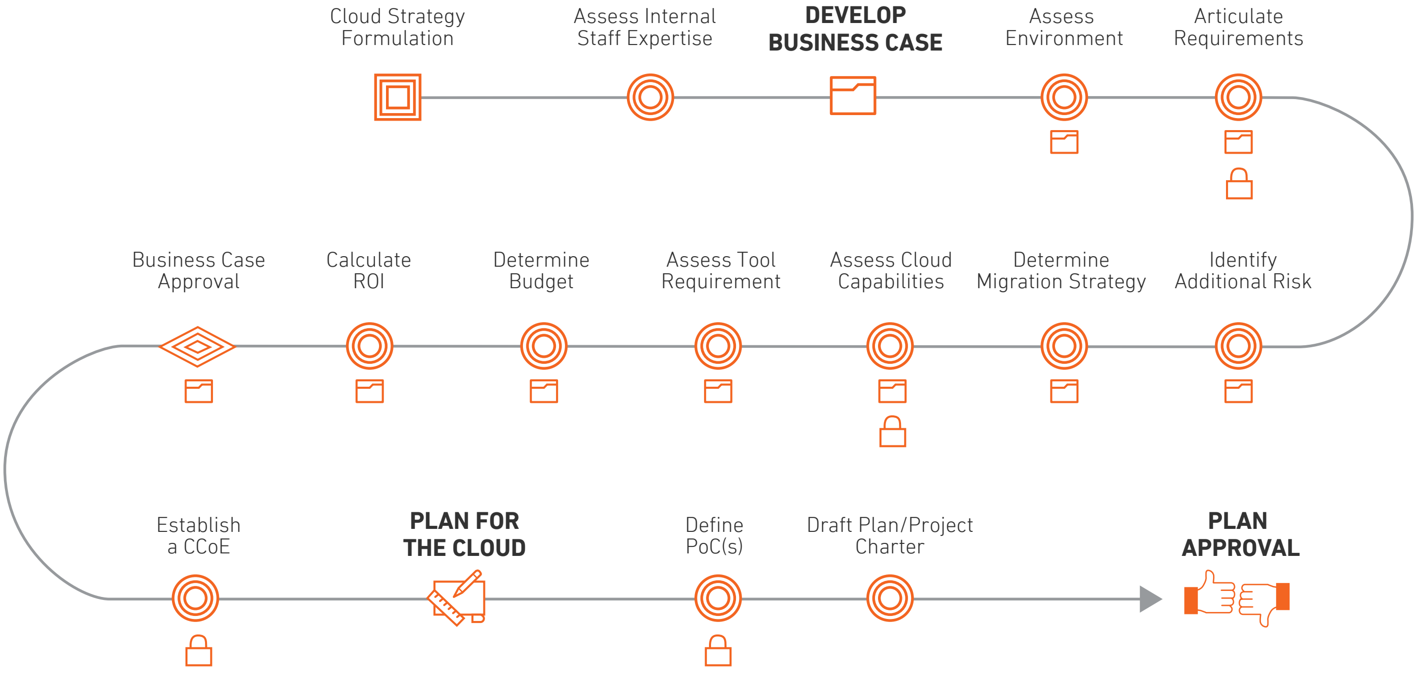
2 VALIDATE

3 BUILD

4 MIGRATE

5 OPTIMIZE

ASSESS & PLAN


Cloud Strategy Formulation
Assess Internal Staff Expertise
DEVELOP BUSINESS CASE
Assess Environment
Articulate Requirements
Business Case Approval
Calculate ROI
Determine Budget
Assess Tool Requirement
Assess Cloud Capabilities
Determine Migration Strategy
Identify Additional Risk
Establish a CCoE
PLAN FOR THE CLOUD
Define PoC(s)
Draft Plan/Project Charter
PLAN APPROVAL

CLOUD MIGRATION ACTIVITIES

DETERMINE YOUR CLOUD STRATEGY

To reiterate, before you take your first step toward migrating applications to the cloud, you need to step back and consider what your organization's overall cloud strategy and policies will be. As the cloud represents a fundamental departure from traditional on-premise IT practices to accelerate the pace of innovation, capture efficiencies, and realize new cost savings, your organization has an opportunity to reap the same from a security and compliance standpoint. In other words, the cloud represents a "do-over" as well as a way to significantly elevate your organization's security and compliance posture.

- Is a "cloud-agnostic" approach important?
- Does your organization require a multi-cloud strategy to meet its needs?
- Do you plan on deploying or expanding current container usage?
- Are you considering deployment for any applications using a microservices architecture?

As we've highlighted in our "11 Strategic Considerations Before Starting Any Migration Project" section, these are just a few of the critical questions to answer as your cloud migration efforts progress.

1. ASSESS STAFFING EXPERTISE

Assess all likely team members who are to be involved in the project. Assess their cloud knowledge, expertise, and direct experience in migrating applications securely to the cloud. Be honest in your assessment. You need to have the right levels and areas of expertise to ensure the success of the project, both in the initial migration and in achieving the return on investment, operational improvements, and the like communicated to leaders. Your realistic assessment should determine whether you should engage a third party for their cloud migration expertise.

DEVELOP A BUSINESS CASE

Develop a business case for the value of migrating workloads to the cloud.

2. ASSESS YOUR ENVIRONMENT

Perform an inventory of your environment, networks, systems, applications, and data to identify and prioritize workloads to be migrated. Look across both production and development environments.

This includes mapping interdependencies between applications and maintaining this information for reference in the design of your cloud architecture. These efforts should also be tied to the actual business processes and importance of those processes to your organization.

If you have access to tools or discovery of your environment, these can be effective in helping identify and map your environment.

3. ARTICULATE REQUIREMENTS

You will want to identify key requirements along the way for each of your workloads and in the context of a broader cloud strategy. Sometimes, individual workload requirements will dictate elements of your broader cloud strategy while other times leadership will have clear mandates as to cloud usage.

Per Workload, identify:

- What cloud platforms (IaaS, PaaS, SaaS) and application hosting, computing performance, and data handling requirements are best appropriate for each workload.
- The scale and importance of applications. (The nature of any impact to customers, impact to business operations, and overall sensitivity to disruption of any kind)
- If the application is a production application or in development.
- Secondary or accompanying processes that might tie to the application and need to be considered as part of the migration.
- Required Operating System versions.
- And assess database services, storage, and ancillary services needed for migration of the application.
- Requirements for supporting multiple geographies.
- Requirements for redundancy.
- Requirements for periods of bursting or dynamic autoscaling based on seasonal, cyclical, or other changes in usage patterns.
- Security controls currently in place that will likely be needed in a cloud environment. For instance, if the application is web-facing, you will likely want to indicate a Web Application Firewall as a requirement.

TIPS

VISIONEERING

Because the cloud represents an entirely different infrastructure and operating model with a growing multitude of capabilities, think about how each workload could be optimized in the cloud, whether your organization chooses to pursue that optimization or not.

EVALUATE EXPERTISE

Before starting down the path of migrating workloads to the cloud, perform a realistic assessment of your organization's experience and expertise to successfully migrate to the cloud. Based on that assessment, you may want to engage a third-party migration partner to help you navigate this complex process.

CAPTURE COST

As you assess your current environment from a technical and business impact standpoint, be sure to assess it from a budget standpoint and capture all costs associated with on-premise and related infrastructure.

CONDUCT SPOT CHECKS

Last, it may be prudent to perform manual spot checks of resources and facility locations to validate asset lists and identify overlooked assets.

- And capture information on access privilege levels and who currently has access to the application. This may be a good time to update any privileges still assigned to former employees, current employees who no longer need access, etc.
- Applicable compliance frameworks across your workloads—ex. PCI DSS, HIPAA/HITRUST, GDPR, etc. Document specific required controls. This step also pertains to frameworks such as NIST and CIS that your organization may use.
- And assess security and compliance control requirements for applications communicating/moving data between cloud and on-premise environments.
- And capture any backup practices for the given application and associated data.

4. IDENTIFY ADDITIONAL RISKS

Perform any last risk analysis and capture as well as benefits analysis for each application or workload. This will be useful in your determination of the appropriate migration strategy as well as useful during the Build phase.

5. DETERMINE MIGRATION STRATEGY

Classify your workloads in terms of suitability for the cloud and what migration strategy to be applied. Consider use of Gartner's 5 R's of Cloud Migration (LINK):

- Rehost (aka "Lift & Shift")
- Refactor
- Revise
- Rebuild
- Replace

TIPS

IDENTIFY GAPS

Be sure to catalog gaps in your assessments as you go. You may find commonalities in needs across applications that the cloud can address.

COMMUNICATIONS

Create a regular cadence of communications on progress for both stakeholders and employees. Use this as a vehicle for change management by helping employees, teams, and others understand the changes taking place and how the organization will need to adapt.

LEVERAGE NATIVE TOOLS

Leverage native cloud tools to lessen the burden of operations. From data warehousing to deployment tools, directories to content delivery, the major public cloud service providers have dozens of tools that may serve your needs.

6. ASSESS CLOUD CAPABILITIES

Once you've completed the assessment of your application and overall environment needs, perform an analysis of the cloud platforms under consideration and the native tools available that may address many of your requirements.

Conduct this assessment and capture results in a way they can be leveraged later through other application assessments you may perform.

Even if your organization is not aware of any current cloud presence, consider use of a discovery tool to identify any Shadow IT that may exist.

As well, be open to how the various cloud options you have may naturally dictate a hybrid or even multi-cloud strategy for your organization.

- Evaluate how your organization can address identity management and role-based access controls with cloud native tools.
- If compliance is critical to your migration, inquire with the cloud service provider as to attestation of compliance with PCI DSS, CSA Cloud Controls Matrix, SOC II, SSAE18, ISO 27001/2, HIPAA, FedRamp, etc.
- Identify and assess native encryption tools the cloud service provider offers.
- Identify and assess native security tools and services the cloud service provider makes available such as AWS CloudTrail, Amazon GuardDuty, Azure Monitor, Azure Security Center, and related Google Audit Logging and Google Security Command Center, to name a few.

Be cognizant of the limitations of these tools. Organizations should still consider how event data and alerting streams will flow into existing security systems and workflows for review by analysts or be used in forensic investigation, in the case of a potential incident.

Cloud native tools have not solved the fundamental problem of security in terms of monitoring and handling (investigation) of alerts and incidents without human intervention.

7. ASSESS TOOL REQUIREMENTS

As you assess the needs of your cloud migration, identify tools that will be necessary based on the cloud migration strategy you selected, and the nature of your application.

- Assess cloud native tools for each potential cloud platform. It may be prudent to capture this information in a way that can be leveraged for other application reviews.
    - ➤ Identify third-party tools that are ready-made for the cloud.
    - ➤ Assess current in-house tools in use that can be leveraged in the cloud. Be sure to validate that licensing permits their usage in your target environment(s).

In effect, this is the beginning stage of designing a Proof of Concept for your cloud application migration.

8. DETERMINE YOUR BUDGET

Assess the overall budget required and Return on Investment. Assess costs associated with your current data center or hosted infrastructure, the cost of tools and licensing, the cost of migration, and the associated cost of the proposed cloud infrastructure solution. This should take into consideration the migration strategy associated with your targeted workload(s).

9. CALCULATE ROI

Calculate the project's Return on Investment. Calculating a Return on Investment is critical given the likely investment involved and expectations by leadership that any large investment provide a return.

APPROVE/REJECT

10. ESTABLISH A CCOE

Once your Business Plan is approved, consider establishing a Cloud Center of Excellence (CCoE) team—essentially a cross-functional migration team—comprised of your IT and migration experts to ensure program and migration success.

Identify and establish access controls and permissions for your cloud migration team members and technical resources involved in migrations.

PLAN FOR THE CLOUD

You now need to take all the insights and requirements you've gathered and begin developing a detailed plan. You'll want to consider whether your cloud migration plan encompasses more than one application and if so, outline multiple streams of cloud migration based on your determinations using Gartner's 5 R's.

You really want to get yourself ready for the actual creation and validation of Proof of Concepts, pilots and the like in support of your cloud migration.

Depending on the nature of your cloud migration strategy for each workload (Gartner's 5 R's), some migration steps may not apply.

TIPS

TRIAL MIGRATION STRATEGIES

Test out each migration strategy using smaller, simpler workload targets first before taking on larger, more complex and critical application workloads. This way, you've identified and documented best practices and potential pitfalls along the way before taking on a much larger project.

TEMPLATIZE

As you plan, think about how you can leverage cloud native tools such as AWS CloudFormation and Azure Resource Manager to create templates that help you and your team more readily deploy applications. Templates can simplify and accelerate the process while also baking in key considerations in terms of security, compliance, and other non-security requirements you may have.

11. DEFINE POC(S)

Design and develop a POC. The POC is intended to validate the feasibility of a workload migration. Your POC should be designed and validated on its ability to address your defined and detailed success criteria.

Though you may not have a POC for every migration strategy, you likely want to consider more than one POC design to address migration for the most complex strategies.

At this point, you are selecting the likely tools you will use for this effort. As such, for any third-party tools, reach out to vendors to determine how they can accommodate your efforts in proving out your migration architecture before selecting and purchasing a given tool.

- Leverage the cloud service provider's partner network for consulting-related services to help you accelerate your proof to value when designing your POC.
- Your POC should reflect security and compliance requirements appropriate to each workload and associated databases and data stores.
- Per the Shared Responsibility model, protection of the actual workloads is the responsibility of the cloud customer. Consider Cloud Workload Protection (CWP) solutions to accelerate addressing this area of responsibility. These solutions typically include:
    - ➤ Host-based IDS
    - ➤ Malware Protection
    - ➤ File Integrity Monitoring
    - ➤ OS Patch Monitoring

12. DRAFT YOUR PLAN/PROJECT CHARTER

At this stage, you need to detail your actual project plan that provides a clear scope and all elements of your cloud migration. This plan should indicate the various sub-projects and sub-tasks, responsible parties, milestones and deadlines, dependencies, risks, and the like. If you are migrating more than one application, you will want to represent sub-streams based on the respective migration strategy selected for each application.

Include planning for communications to stakeholders and others across the organization.

You will also want to capture budget information broken down across your plan as appropriate. As well, define clear Key Performance Indicators (KPIs) and other metrics for program performance.

In terms of roles and responsibilities, detail a RACI chart for the project. And your plan should not move forward without capturing information on needed skill sets and expertise within the organization.

For instance, include any hiring or training for the following:

- Cloud Architect
- Cloud Automation Architect
- Cloud Engineer
- Cloud Services Developer
- Systems Administrator
- Cloud Security Architect
- Cloud Software and/or Network Engineer

Finally, depending on the breadth and complexity of your overall project, you may want to consider assigning a Project Manager to program manage the effort.

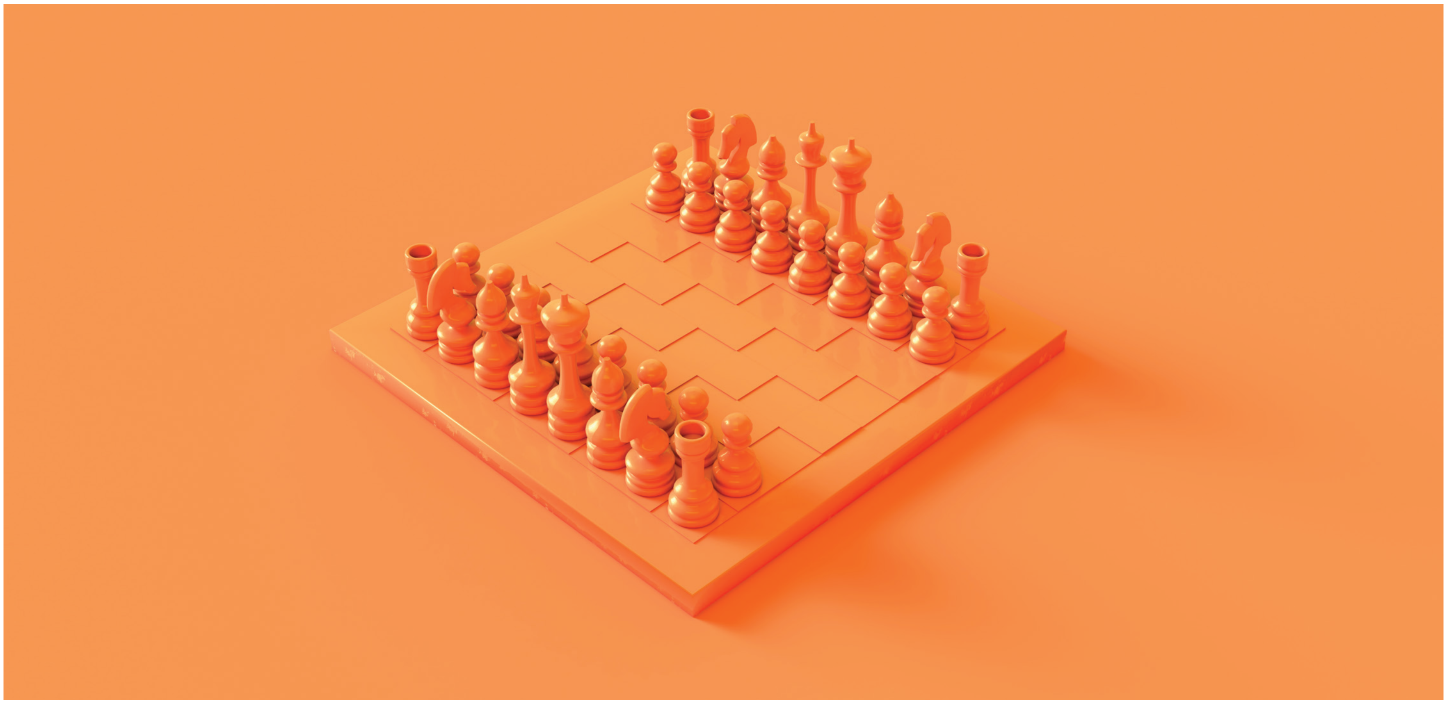
You should not leave the Assess & Plan phase without this plan in place, approved by stakeholders and/or your CCoE team.

TIPS

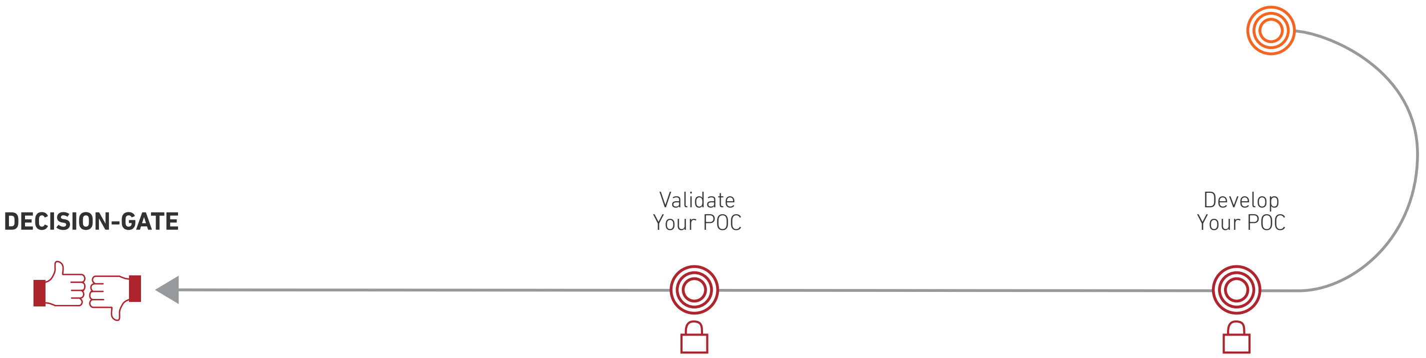
IDENTIFY KPIs

Before you fully migrate a targeted workload to the cloud, be sure to articulate Key Performance Indicators (KPIs) that will govern success of your pilot as well as your full production rollout. When crafting KPIs, consider your original business case and the factors for how Return on Investment was based. The closer you can tie KPIs to your ROI model, the better.

PLAN APPROVAL



VALIDATE



DECISION-GATE

Validate
Your POC

Develop
Your POC

CLOUD MIGRATION ACTIVITIES

Depending on the nature of your cloud migration strategy for each workload (Gartner's 5 R's), some of the areas mentioned here may not apply.

1. DEVELOP YOUR POC(S)

Develop your Proof of Concept. The POC is intended to validate the feasibility of a workload migration. Your POC should be designed and validated on its ability to address your defined and detailed success criteria.

- From the start, ensure that your organization follows best practices for secure code development of applications. OWASP, or the Open Web Application Security Project, provides detailed information on best practices.

The Security Knowledge Framework also provides free resources to aid in secure code development.

- When developing and validating your POC, ensure that you are leveraging the Well Architected Framework and focus on the Security Pillar to adhere to best practice methodologies for controls and standards considerations. When an Attestation of Compliance (AOC) is a requirement for your business function, investigate the underlying regulatory frameworks the cloud provider maps to, and understand any ancillary responsibilities you must adhere to as a tenant of their cloud. The necessary controls may be satisfied with native cloud services, but also may require partner solutions to fill any gaps.
- Are any IT Security and/or DevOps practitioners responsible for the security and compliance part of your Proof-of-Concept design? They have a vested interest as well, because automated tools only go so far. These teams are likely the ones to manage and monitor security for your migrated applications after your migration project is long over.
- Be sure to incorporate security and compliance controls and tools as part of your Proof of Concept.
- Regardless of the state of your POC, employ multi-factor authentication.
- Employ encryption for both data in transit and at rest.
- Implement Cloud Workload Protection for your application workloads in the cloud.

2. VALIDATE YOUR POC(S)

Validation is a critical step and should not be taken lightly. You want to validate that the Proof of Concept for each application (where applied) you are migrating to the cloud meets key requirements across a number of categories.

Business Requirements

Does the POC address the key business drivers behind the push to leverage the cloud? What apparent benefits does the POC indicate?

Customer Requirements

Are there specific customer requirements the POC should satisfy?

Operational Requirements

Does the POC meet operational requirements for how the application will perform to enhance productivity, increase efficiencies, or drive operational improvements, etc.?

Performance Requirements

Does the POC indicate that performance targets will be met or exceeded? How do performance measures suggest that performance can be even greater than that previously measured?

Security and Compliance Control Requirements

Does the POC provide a strong defense-in-depth security posture while addressing appropriate compliance controls? Do security and compliance controls appear to be operating effectively? Does the POC reflect an enhanced future-state for security and compliance in the cloud?

Security Operational Requirements

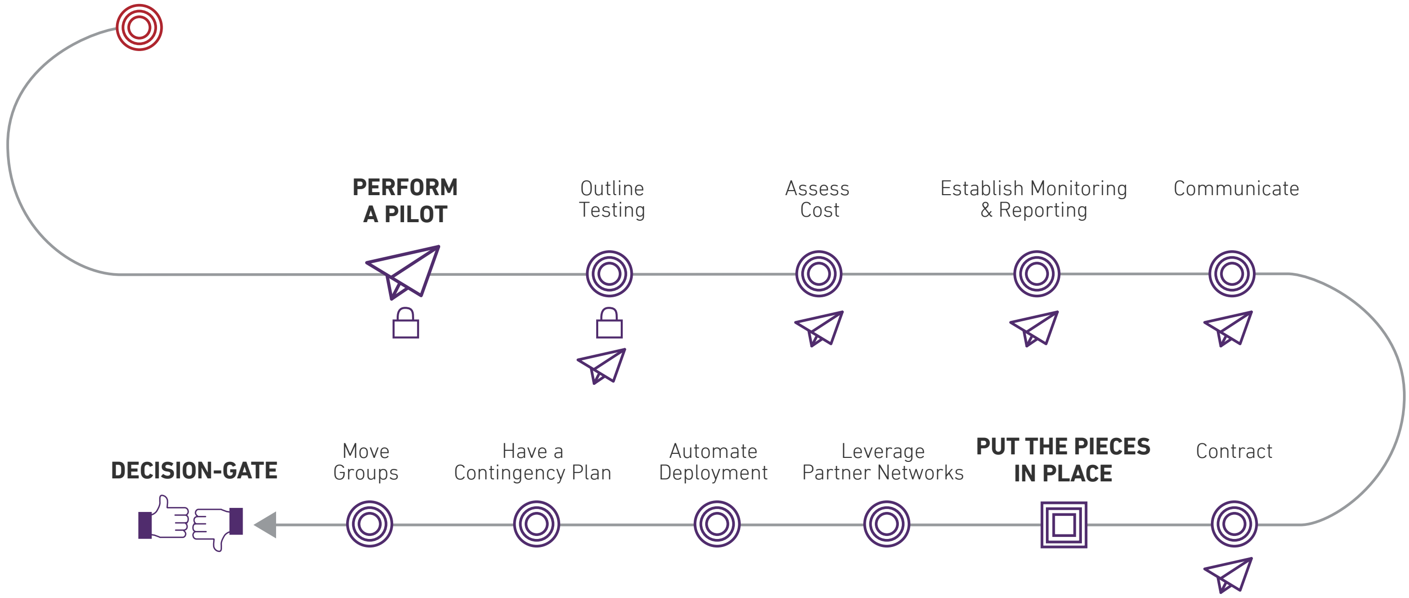
Does the POC address integration of logging and event information into existing security processes and workflows? Do existing Security, Compliance and DevOps personnel have visibility to monitor activities taking place across your applications in the cloud 24/7/365, as well as have the right tools and access to investigate and act on areas of concern?

Cost Requirements

Does the POC suggest that cost targets will be met or even exceeded, and that the organization will likely obtain its proposed return on investment?

DECISION-GATE

BUILD


PERFORM A PILOT
Outline Testing
Assess Cost
Establish Monitoring & Reporting
Communicate
DECISION-GATE
Move Groups
Have a Contingency Plan
Automate Deployment
Leverage Partner Networks
PUT THE PIECES IN PLACE
Contract

CLOUD MIGRATION ACTIVITIES

PERFORM A PILOT

More extensive than a POC, use a pilot as a "near production" implementation of your workload in the cloud. The pilot is based on your detailed cloud architecture diagrams, requirements, and the like. The pilot should be extensively validated both by internal users and then by a select user base of your customers or other consumers.

- From the start, ensure that your organization follows best practices for secure code development of applications. OWASP, or the Open Web Application Security Project, provides detailed information on best practices.
- The Security Knowledge Framework also provides free resources to aid in secure code development.
- Ensure that Security, IT, and/or DevOps teams responsible for overall security of your applications in the cloud are engaged prior to pilot deployment.
- Implement Identity and Access Management policies. Setting who has access and what levels of access to a given workload is vital. You need to establish (based on your identified requirements in the Assess & Plan stage) what privilege levels of access are needed, who should have access to what level, and how you will monitor for indications that access has been compromised.
- Hash and salt any databases that contain user login credentials. Put in place behavior and anomaly analysis to detect and alert on unusual log-in attempts or unusual access.
- Implement a Patch Management methodology that scans applications and patches to eliminate vulnerabilities as early as possible in the DevOps cycle. Use a vulnerability classification schema or third-party service to prioritize vulnerabilities based on their likelihood of exploitation. Perform testing before any rollout of patches into production.
- Employ Multi-Factor Authentication (MFA) practices.
- Employ encryption for the application and data.
- If using APIs, perform testing to validate that APIs are secure.
- Implement Cloud Workload Protection for application-level attack monitoring of your application workloads in the cloud. CWP protection typically addresses critical security and compliance controls:
    - ➤ Scan for and patch vulnerabilities in your application. Ideally, vulnerability scanning should be done for both production applications and on development applications as early in the DevOps cycle as possible.
    - ➤ Implement detection of and protection from malware for your instance.

  - ➤ Implement File Integrity Monitoring to monitor for and alert on changes to OS registries, application files, etc.
  - ➤ Implement host-based IDS for analysis of traffic and detection of potential threats.
- Some CWP protections can also be extended to protection of containerized applications.
- Validate that any new technologies or tools do not present new security risks to your overall application. Ensure that any necessary event or log information (if applicable) is flowing into security workflows for analysis.
- If using third-party software, ask the vendor for detailed documentation on their own security practices to ensure no additional vendor-related risk is introduced into your overall application environment. Consider creating a "coverage matrix" to identify all third-party, and cloud native tools, in use and document what security and compliance controls are in place to protect this overall vendor supply chain.
- Ensure that monitoring and associated staffing is adequately in place to support required security and compliance outcomes.
- Implement an appropriate backup policy and regimen. You may want to consider a 3-2-1 strategy. Besides your active copy, one backup could be on a different media with the same provider while another copy is located at an off-site location such as on-premise or even with another cloud service provider platform.
- Run a posture assessment. At this point, it is prudent to run a Cloud Security Posture Assessment to evaluate controls across the workload, databases, and storage in use. Be sure to assess against any appropriate compliance framework if the workload and related data are subject to these guidelines.
- Validate that all security and compliance controls are operable and event telemetry is being received and is visible to in-house or outsourced security teams for monitoring and analysis.

1. OUTLINE TESTING

Don't wait until your actual application is migrated over to outline what testing needs to take place to ensure all is operating as it should. Go ahead and identify required areas of testing, who is responsible, and when testing must be completed by.

Consider testing across:

- Application Testing
- Infrastructure Testing
- Usability and User Acceptance Testing
- Performance Testing
- Security and Compliance Testing

2. ASSESS COST

Pay careful attention to compute and data usage and associated cost to identify strategies to reduce overall cost of running your workloads.

3. ESTABLISH MONITORING AND REPORTING

Build in appropriate mechanisms for monitoring and reporting of the application.

4. COMMUNICATE

When performing your pilot, alert stakeholders and others who are impacted directly or indirectly by the application that a pilot is being conducted and for them to alert your team should any issues arise.

5. CONTRACT

When contracting for additional tools and services, you will want to prove your migration solution before doing so. This is part of managing risk—you want to be careful about commitments before you've proven out your approach.

Because not every vendor will allow "trial" periods, consider short-term usage agreements to insulate your efforts from being locked into a vendor that may not make it through the Validate and Build stages. Fortunately, many of the tools you may need are cloud-based and offered as security-as-a-service, which generally means more flexibility in short-term usage and billing.

6. PUT THE PIECES IN PLACE

You've validated your Proof of Concept and even conducted a successful pilot by this stage. It's time to solidify your solution.

This includes establishing necessary vendor relationships, acquiring/contracting for tools, establishing SLAs, etc. It also includes turning up the various cloud-native tools you've selected.

7. LEVERAGE PARTNER NETWORKS

Take advantage of the various cloud partner networks such as AWS Marketplace, Azure Marketplace, and Google Cloud Platform Marketplace. These networks catalog the spectrum of computing power, storage, networking, and databases on demand. In addition, these networks are filled with security partners, cloud migration, transformation consultants and tools, and cost-optimization and monitoring organizations to help operate in the cloud successfully.

In addition, purchasing through the marketplaces can simplify vendor management and tool and services acquisition because services can be consolidated under the Cloud Service Provider's "paper."

8. AUTOMATE DEPLOYMENT

As you build the infrastructure and incorporate cloud-native and third-party tools necessary for your targeted workload migration, you will also want to focus on creating automated deployment scripts or templates that will help with the actual migration process.

9. HAVE A CONTINGENCY PLAN

You need to think through both the most likely and the worst-case scenarios that could occur during your migration, and draft contingency plans for these eventualities should they occur.

You should already have a sense of the business impact of any type of disruption and even may have conducted a formal business impact analysis as part of your initial application assessments. Use this to formulate appropriate BC/DR planning, including the ability to roll back the application, if needed.

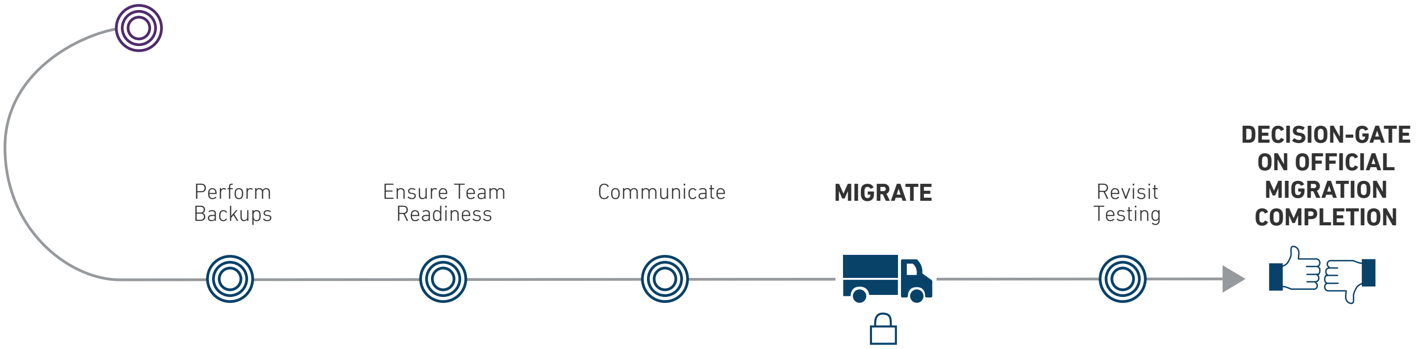
Last, be in touch with your Marketing and Customer Communications team to alert customers should any issues arise associated with the application.

10. MOVE GROUPS

Depending on the overall scope of your project, in terms of the number of workloads being migrated, you may want to identify groups of applications for movement at the same or near time.

DECISION-GATE

MIGRATE


Perform Backups
Ensure Team Readiness
Communicate
MIGRATE
Revisit Testing
DECISION-GATE ON OFFICIAL MIGRATION COMPLETION

CLOUD MIGRATION ACTIVITIES

1. PERFORM BACKUPS

Perform backups for applications, associated databases, and stored data, as well as for any ancillary services tied into the migration project.

Make sure backups are as near real-time as possible depending on the use case and sensitivity of your application.

2. ENSURE TEAM READINESS

Confirm that the team is ready to support the migration and jump in should any issues arise.

This includes having appropriate IT, Security, and DevOps teams engaged to work with the migration team on any immediate changes that are necessary.

3. COMMUNICATE

Take time to communicate to all stakeholders, employees, and others inside the organization that could be directly or indirectly affected by the migration. Enlist their help to evaluate performance and provide a direct way for these groups to communicate any issues they come across or are alerted to.

4. MIGRATE

All aspects of security and compliance covered in the Build phase would likely be the same for the Migrate phase.

- Implement a Cloud Security Posture Management Solution.
- Put in place a CSPM capability for automated discovery, assessment, and remediation of security and compliance controls across your cloud footprint.
- Implement a Patch Management methodology that scans applications and patches to eliminate vulnerabilities as early as possible in the DevOps cycle. Use a vulnerability classification schema or third-party service to prioritize vulnerabilities based on their likelihood of exploitation. Perform testing before any rollout of patches into production. Ideally, your ultimate goal is that your production applications are based on a trusted image and no updates or patches to the production application itself is performed.

- Employ Multi-Factor Authentication (MFA) practices.
- Implement Identity and Access Management policies. Setting who has access and what levels of access to a given workload is vital. You need to establish (based on your identified requirements in the Assess & Plan stage) what privilege levels of access are needed, who should have access to what level, and how you will monitor for indications that access has been compromised.
- Employ encryption for the application and data.
- Segment application data from other applications based on data classification schemes you may have in place.
- If using APIs, perform testing to validate that APIs are secure.
- Implement Cloud Workload Protection for your application workloads in the cloud. CWP typically addresses critical security and compliance controls:
    - ➤ Scan for and patch vulnerabilities in your application. Ideally, vulnerability scanning should be done for both production applications and on applications in development as early in the DevOps cycle as possible.
    - ➤ Implement detection of and protection from malware for your instance.
    - ➤ Implement File Integrity Monitoring to monitor for and alert on changes to OS registries, application files, etc.
    - ➤ Implement host-based IDS for analysis of traffic and detection of potential threats.
- Some CWPs can also be extended to protection of containerized applications.
- Centralize logging to meet compliance requirements and enhance security analysis and correlation.
- Validate that any new technologies or tools do not present new security risks to your overall application. Ensure that any necessary event or log information (if applicable) is flowing into security workflows for analysis.
- If using third-party software, ask the vendor for detailed documentation on their own security practices to ensure no additional vendor-related risk is introduced into your overall application environment. Consider creating a "coverage matrix" to identify all third-party, and cloud-native tools, in use, and document what security and compliance controls are in place to protect this overall vendor supply chain.
- Ensure that monitoring and associated staffing is adequately in place to support required security and compliance outcomes.
- Once the application has been migrated, you may want to consider performing a penetration test based on the nature and sensitivity of the application. Be sure to incorporate the cost of penetration testing into your budget as well as timelines if you plan on using an external third party for the testing.

- Depending on the sensitivity of the application, implement protection against Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS)attacks. Evaluate native tools the cloud service provider may have that can be applied for this purpose.
- Depending on the sensitivity of the application and data it touches, implement Data Loss Prevention (DLP) to monitor for potential data leakage across your cloud environment.
- Because social engineering still represents a threat vector that can allow actors to gain "legitimate" access credentials to an application, be sure your IT and/or Security team is conducting employee security awareness training to reduce the likelihood of employees falling prey to social engineering emails, calls, and other efforts.

5. REVISIT TESTING

Perform testing of your migrated application based on what was outlined during the pilot phase. You may want to expand testing given the actual application is now fully migrated, and you want to be sure all aspects are operating as intended.

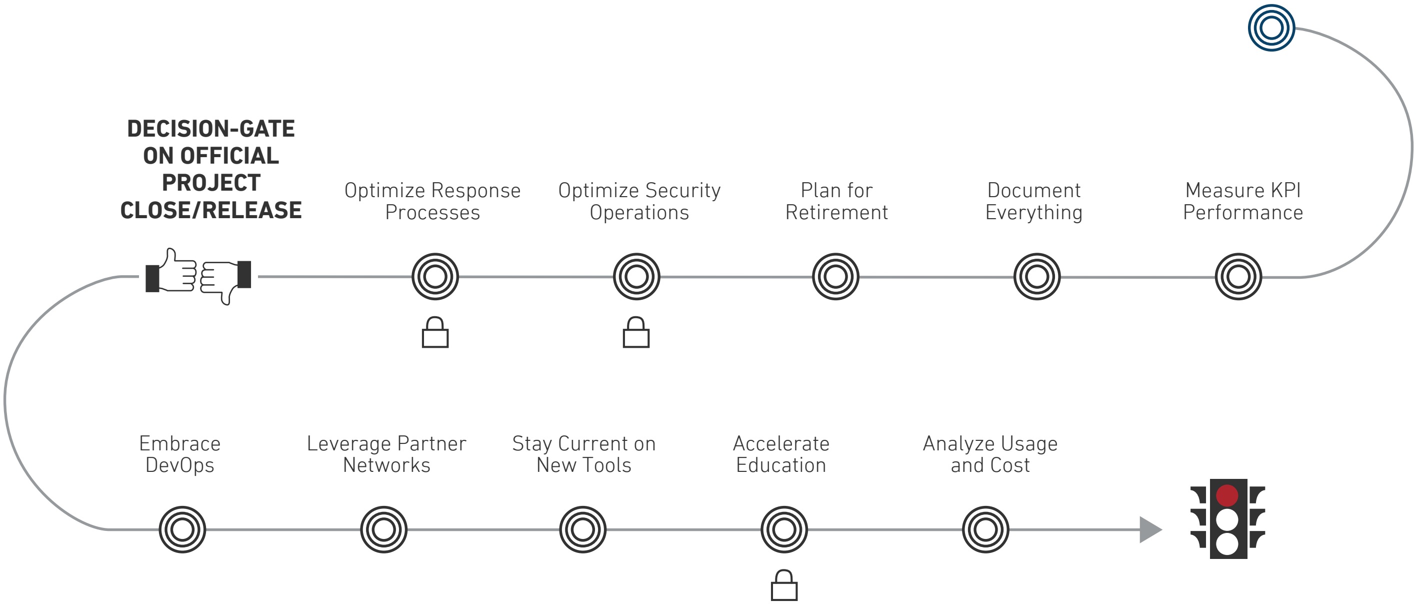
Consider testing across:

- Application Testing
- Infrastructure Testing
- Usability and User Acceptance Testing
- Performance Testing
- Security and Compliance Testing

Also have your team on standby to take in and address user issues that may arise from the implementation.

DECISION-GATE ON OFFICIAL MIGRATION COMPLETION

OPTIMIZE


DECISION-GATE ON OFFICIAL PROJECT CLOSE/RELEASE
Optimize Response Processes
Optimize Security Operations
Plan for Retirement
Document Everything
Measure KPI Performance
Embrace DevOps
Leverage Partner Networks
Stay Current on New Tools
Accelerate Education
Analyze Usage and Cost

CLOUD MIGRATION ACTIVITIES

1. MEASURE KPI PERFORMANCE

Begin measuring and reporting on KPI performance at the earliest moment possible for each measure. Perform root-cause and other analysis for any KPIs not performing to expectations and take appropriate action to address.

2. DOCUMENT EVERYTHING

Document best practices, processes, tools, and templates from the project as a guide for conducting future migration projects and at a more accelerated and efficient pace. Do this for each cloud platform used, as appropriate, and for each cloud migration strategy (Gartner's 5 R's).

3. PLAN FOR RETIREMENT

To ensure you capitalize on your project ROI, you need to make certain you finish the mundane work of decommissioning systems, software, and related sites.

- Decommission impacted assets.
- Process assets through reuse, resale, donation, and scrap (per Corporate Investment Recovery best practices), as appropriate.
- Make sure to update systems like SAP and other financial systems of record to reflect decommissioned capital assets.
- Perform actions or release to Facilities Management to render the site back to original condition per leasing agreement or other plan.
- Relinquish site control.

4. OPTIMIZE SECURITY OPERATIONS

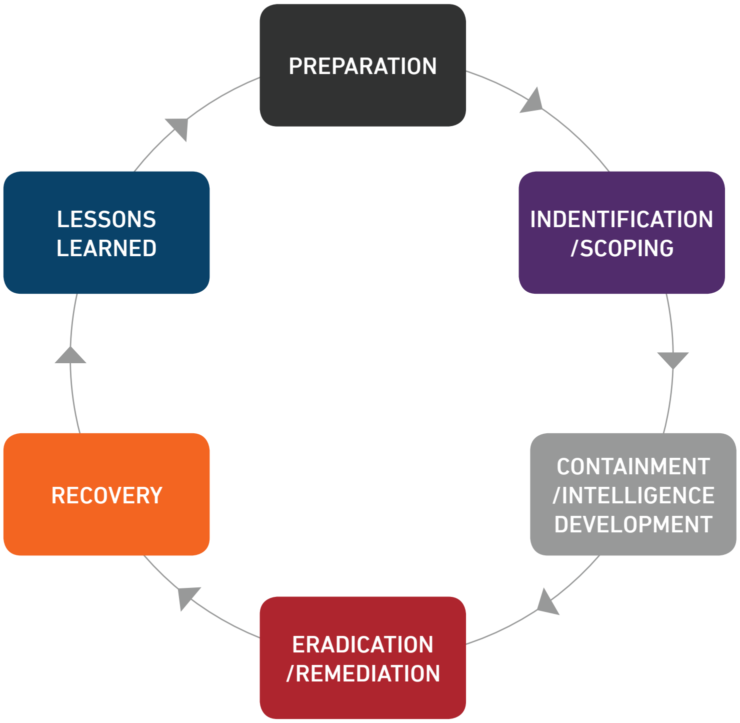
Perform analysis of security operations related to each application to date in order to identify areas for tuning and optimization.

- Assess privilege levels and review who has access.
- Analyze logs looking for unusual access and activities.
- Analyze alerting and alert triaging to identify ways to reduce alert volume and fatigue.
- Measure False Positive rates and establish other indicators for assessing performance.
- Analyze vulnerabilities to identify areas for improvement.
- Tune and optimize security controls such as firewalls, Web Application Firewalls, IDS, etc.

5. OPTIMIZE RESPONSE PROCESSES

IT/Security and DevOps teams need to thoroughly document Incident Response practices for any incident affecting applications and data in the cloud.

- Document in your Incident Response Plan how the organization will respond to incidents in each cloud environment.
- Leverage cloud-native tools that can aid in forensic investigation and response.
- Capture learnings from each incident investigation, including the nature of the threat vector, targeted applications and data, type of threat actor (if identifiable), as well as post-remediation steps implemented to prevent threat actor re-entry.
- For perspective, 43.6% of survey respondents indicated that they believed their organization has suffered a breach from the same threat actor on more than one occasion, according to the 2018 SANS Incident Response Survey.
- Consider mapping each incident to the Cyber Kill Chain® (by Lockheed Martin) or kill chain model you prefer.
- Track false positives and document action taken to develop rules, countermeasures, and other controls to prevent their reoccurrence in the future.
- Collect and store logs (for at least 1 year to aid in forensic analysis, if needed).
- Leverage tools that can automate processes and even orchestrate remediation of issues based on pre-defined guidance.
- Based on the sensitivity of your environment, applications, and data, consider performing Red Team exercises to assess security and compliance controls against a trusted adversary.



PROJECT SIGN-OFF

Collect and report on all indicators and overall success of the project to stakeholders once complete. This includes the cost savings/avoidance realized as well as performance and efficiency gains. The status of your return on investment should be front and center. Get sign-off to officially close the project and release personnel and facility/asset resources.

Because some indicators may have yet to be fully realized, plan to continue monitoring results and report to stakeholders in the future.

POST-PROJECT

6. EMBRACE DEVOPS

Embrace DevOps in the cloud. DevOps offers you the tools and ability to deliver applications and services faster, giving you a competitive edge over organizations using traditional software development and infrastructure management processes. It's important to build security into your DevOps capabilities right from the start, making it an integral part of your infrastructure rather than an add-on capability.

7. LEVERAGE PARTNER NETWORKS

Take advantage of the various cloud partner networks such as AWS Marketplace, Azure Marketplace, and Google Cloud Platform Marketplace. These networks catalog a range of potential security and compliance partners, cloud migration and transformation consultants, and tools and solutions to help you securely migrate and optimize your operations in the cloud, securely.

8. STAY CURRENT ON NEW TOOLS

Cloud technology is continually evolving, providing organizations with new capabilities and tools. Stay on top of what the cloud offers through research by your own team and by relying on trusted partners to alert you to new capabilities available in the cloud.

9. ACCELERATE EDUCATION

Drive toward greater cloud knowledge and expertise by having staff take advantage of both free training provided by major cloud service providers as well as premium training content and conferences. To that end, budget for paid training over the next 12 months to enhance cloud comprehension and skill sets.

- Education should also encompass a focus on cloud security and span IT/Security and DevOps teams.

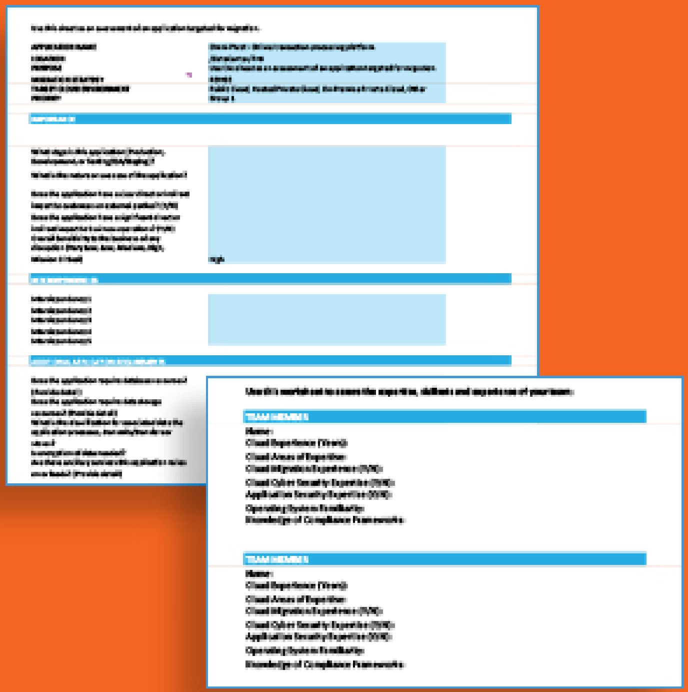
Note: Training should drive toward having strong cloud and cloud security competencies on staff, and not on just a generalized understanding of the cloud.

10. ANALYZE USAGE AND COST

Perform analysis on usage and associated cost to identify areas where cost performance can be optimized. This is especially important as waste can be as high as 35% as cited by RightScale in its 2019 State of the Cloud Report.

ACCELERATE YOUR SECURE CLOUD MIGRATION EFFORTS

Get the Secure Cloud Migration Template



SOURCES

The following sources were researched in the development of this guide.

Security and Compliance perspectives, as well as additional perspectives on cloud migration, are provided by Armor Cloud Security.

"The AWS Cloud Adoption Framework," Amazon Web Services

Azure Migration Center, Microsoft

Migration Center, Google

"Security Knowledge Framework," OWASP

"The Dirty Dozen: 12 Top Cloud Security Threats," CSO Online – Bob Violino – June 11, 2019

"RIGHTSCALE 2019 STATE OF THE CLOUD REPORT FROM FLEXERA™" Flexera – 2019

"Tips For Building a Cloud Migration Plan," Chris Rechtsteiner - ServerCentral – November 5, 2018

"5 Tips to Ensure a Secure Cloud Migration," Gilad David Maayan - Security Boulevard – October 15, 2018

"Cloud Migration Checklist for Application and Data Security," Imperva – January 29, 2018

"Hybrid Cloud Drives Growing Container Production Use and Disruption," 451 Research, May 2017

"Containers: Real Adoption And Use Cases In 2017," Forrester – March 2017

"The 5 Phases of Cloud Transformation," Pythian – Robert Weiss – 2016

"Intelligence Concepts – The SANS Incident Response Process," Scott J. Roberts – March 17, 2015

"Migrating Applications to the Cloud: Rehost, Refactor, Revise, Rebuild", Gartner – December 3, 2010

ARMOR

ARMOR.COM | (US) +1 844 682 2858 | (UK) +44 800 500 3167