Guide to enterprise cloud adoption

Addressing the five most common concerns
# TABLE OF CONTENTS

**EXECUTIVE SUMMARY** 03

---

1. WHY IS YOUR ENTERPRISE GOING BIG ON CLOUD? 04

---

2. WHAT WILL IT TAKE TO LEAD MY TEAM THROUGH TIMES OF CHANGE? 05

---

3. HOW CAN I ACCELERATE MY CLOUD PROGRAM WITHOUT PUTTING MY ORGANIZATION AT RISK? 07

---

4. WHAT MUST I DO TO ENSURE SECURITY IN MY CLOUD PROGRAM? 11

---

5. HOW CAN I UNLOCK CONTINUOUS INNOVATION ONCE MY TEAM IS OPERATING IN THE CLOUD? 14

---

**CONCLUSION** 16
Executive summary

Whether you are leading through times of change, ensuring security or adopting a DevOps mentality, we address your top concerns and offer industry best practices proven to accelerate your cloud program.

You may be faced with the challenge to go big on cloud or take on a cloud-first mandate. Deciphering where to start or what elements to include or what guidance to follow can be the hardest part of that challenge. How do you separate the marketing hype from evidence gathered from credible sources? How do you know you are getting information that can really help? Our goal is simple—to help you accelerate your program by giving you the framework of best practices we have found that work. Yes, it is possible for an enterprise to reach the promised land of cloud adoption quickly and in control, and we assembled the framework you can put into practice today.

This guide outlines what is required to build your cloud program by answering some key questions critical to your success:

1. Why is your enterprise going big on cloud?
2. What will it take to lead my team through times of change?
3. How can I accelerate my cloud program without putting my organization at risk?
4. What must I do to ensure security in my cloud program?
5. How do I unlock continuous innovation once my team is operating in the cloud?
1. Why is your enterprise going big on cloud?

The **why** of cloud is agility. For some, agility means survival while for others it means greater prosperity. No one likes living in reaction mode; therefore, going big on cloud should be a mandate. It is about having the courage to chart a new course and owning your destiny.

Moving fast is now the mantra of every business unit and central IT group worldwide. Cloud-native applications are enabling small, efficient teams to compete head to head with established multibillion-dollar enterprises, which often results in the complete disruption of their well-defended markets. Without the burden of legacy people, processes, and technology, the born-in-the-cloud team will do more in less time and for significantly less money.

When we speak of going big on cloud, we are referring to the adoption of attitudes and actions that enable the business to move at speed while controlling risk. Going big is a leadership construct that requires a vision unlike any other vision. We must see what is possible and lead our teams to the goal—cloud makes much of it possible. Going big on cloud is also a mandate of technology. Similar to, but much larger than the PC and internet movements, the cloud—specifically automated infrastructure—is now the baseline.

The achievement of agility is, in part, through the adoption of clear and prescriptive processes and technology. With the enablement of technology speed through automated infrastructure and IT resources, developers can provision every operational support feature necessary to release their application—in code. The staggering speeds by which systems are deployed have literally reshaped our industry—never to return in shape or form.

Therefore, the **why** of cloud is speed. Ask yourself—is the purpose of your program speed? Are there others who want to go big on cloud for cost? Be careful, cutting costs using cloud is tricky and is not sustainable as a competitive advantage. Flexibility, speed, and the ability to resound to market needs are significantly more beneficial. Don’t lose focus on this critical fact.
2. What will it take to lead my team through times of change?

When we speak of going big on cloud, we are referring to the adoption of attitudes and actions that enable a business to move faster while controlling risk. Cloud makes organizations more agile. With cloud, iterations and changes occur more frequently than ever before. This generates huge benefits for the company as a whole, helping it enter new markets, meet customer demands better, and be more competitive. But these changes also impact people. Changes in job titles, responsibilities, and even hours of work may not happen all at once or reach all corners of the organization at the same time. But what is certain is that a transition to cloud will eventually bring about more change. Going big is a leadership construct that requires a vision unlike any other. As a leader, you must see what is possible and lead your team to the goal.

Your cloud program must include a strong leadership component, specifically around how people’s roles will evolve. When the vision of the future is not clear, people get scared and make bad choices. Your goal is to provide clarity at every step. You cannot over communicate in your cloud program. Here are key communication functions you'll want to implement:

1. **Lift team value:** Managing employees during a cloud transition involves much more than just learning new technical skills. In the cloud, the entire way things are done is different. Going from a waterfall-type project management model to agile, Scrum, DevOps, and Continuous Delivery represents a very new way of operating. Tools, resources, and training must be provided so your team can deliver on the promise of cloud. Without the tools and resources to do the job, the team's value does not feel supported. This is when they fracture and stop acting like a team. As a leader, your top communications priority is to clearly articulate training plans and enable your team by providing them with what they need to get the job done.
2. Be clear on roles and responsibilities:
Seventy percent of change initiatives fail because the people part of the equation is left out. Leaders have to explain clearly to a person that their move to become a cloud technologist will involve changes in their work process, title, and role in the organization. When change happens, the person needs to know what is changing, how it is changing, and why it is changing. Specifically, employees need to know what you want them to stop doing, start doing, and continue doing. Also, when it comes to cloud, retraining is a given. It costs a lot to hire someone new and upskill them. So, if you already have a team, make sure you are managing that talent to the best of your ability. Communicate your enthusiasm for the new roles and how the new positions will benefit them. Focus on building confidence and motivating the individuals to want to do this new job.

3. Lead the way with mentors: Every team wants to succeed, but when a team is tasked with a new, broad project, it’s hard to anticipate the little things that may pop up. Working in a vacuum, teams can get derailed and make choices that put the project at risk. Cloud breaks down silos, requiring employees to work with business units they may not have interacted with before. Employees must learn how to engage in a cross-functional team with new people and unfamiliar skill sets. As a leader, explain why you are bringing in a consulting partner and experts who have done this before and can mentor the team. They are not here to stay but to guide. It is an insurance policy against project failure.

4. Make it safe to try: The team needs protection. Agility is about rapid failure and discovery. A team may iterate on a project 20 or 30 times in a short period before they get version 1.0 right. When using cloud platforms appropriately, the risk and cost of failure is dramatically lowered. However, your leadership mindset must change to enable a culture of trust and to encourage a fail-fast mentality. That means it must be safe to try new avenues, new technologies, and new ideas. If the team does not have significant executive trust, agility and innovation will die because the team fears failure. You must communicate this fact and demonstrate it in your actions.

Although cloud enables agility and rapid change, a transition to the cloud takes time. To get where you need to go, you have to create a plan and make sure you are pushing forward on all fronts—leveraging the right tools, acquiring the right resources, and configuring the organization to compete in the new environment. People are a critical part of the plan and are very often the key to its success or its failure. There is no clear cutover for a team, and managers need to dedicate time and effort to the individual transitions their employees are going through to help them move along the path to success.
3. How can I accelerate my cloud program without putting my organization at risk?

Agility means the ability to move quickly and easily. Going fast in the cloud is about teaching your teams to adopt processes and technologies that are not common in today’s enterprise IT universe. You are going from a waterfall process to one that enables iteration on infrastructure code. For many, the approaching storm of cloud computing is anything but quick and easy. The vast array of technology choices and their implications often stop decision-makers in their tracks. At that point, the goal of agility is lost in the IT paralysis of not wanting to make a bad decision.

Here are ten accelerators you can do now, that cut months from your project, helping you realize value sooner.

1. **Naming and tagging:** Naming and tagging provides an easy way to assign metadata to cloud resources. Tags are ubiquitous in the cloud ecosystem of tool vendors. Therefore, **having a solid tagging structure from day one is critical.** It enables the rapid inclusion of tools without having to sort out how they interact with each other. Take note, learn how the tags are used, and create a tagging strategy; otherwise, you could create quite a mess in a very short period of time. This step is a mandate. Do not skip it, and more importantly, enforce your tagging practice from day 1!

2. **Tool selection and strategy:** Teams must consider a new array of tools for building a secure and robust cloud environment that meets their needs. These include IAM, IPS, IDS, directory services, endpoint protection, backup, incident management, logging and monitoring, and a whole host of functions. Without the knowledge of how these tools interact, handle scaling, and auto-recover from a failure, you could waste a solid year of time. Your tool strategy must be road tested and include a prescriptive list of tool providers who solve specific functions in a highly agile, highly available manner. Do not be fooled by cloud-wasted vendors who have taken their on-premises tools, lifted and shifted their software, and called it cloud enabled. Make sure each tool is cloud-native, can handle pay-per-use consumption, and is HA ready.
3. **Patch management**: Similar to on-premises, OS images and tool components must be updated with patches regularly. Your patch management practice should leverage an automated framework that ensures all applications and tools are running on your approved OS images. More importantly, the framework underlying the patching process should be a combination of detection and remediation, as defined by the release standards of your organization. Patch management is absolutely critical to agility. The right tools enable faster cloud adoption by ensuring the OS images are always compliant. Done right, this Day 1 activity results in a platform that both the development and security communities can trust. Therefore, make sure the developers and app owners are building their apps from an approved repository of server images.

4. **Cloud account structure**: On the surface, accounts are a good way to enforce separation of environments. They enable separate billing, provide hard firewalls between business units, and offer clear ownership of resources. However, they do tend to get out of hand rapidly. The major cloud providers offer a variety of services and features that allow for flexible control of cloud-computing resources and the account(s) managing those resources to help you avoid account sprawl. These options are designed to help provide proper cost allocation, agility, and security. However, sometimes it can be challenging to understand how best to implement an account structure strategy—especially when working with multiple, even hundreds of, accounts. Each organization is different, and cost allocation, management of budget, and separation of systems are always critical in the implementation process.

5. **IAM policies and roles**: Identity and Access Management (IAM) is the cloud version of your user identity credential system. IAM policies and roles provide a security approach and technology that enables the right individuals to access the right resources, at the right times, for the right reasons. It follows the principles that everything and everyone gets an identity; this includes humans, servers, APIs, applications, data, and others. Once that verification occurs, it’s just a matter of defining which identities can access other identities, and creating policies that define the limits of that relationship. Getting your users and groups sorted out can be tricky business and will block the agility play without a proper methodology for control. Alignment with all the tools, roles, and users is critical for Day 1.
6. **Encryption and key management:** The major cloud providers offer a key management system (KMS) as a service, for the seamless, centralized control over keys used to encrypt data on the cloud. KMS gives options for data protection, and features for scalability and availability when implementing key management at enterprise scale. The combination of processes and technology must be sorted out before launching any service. Without the automation to process the data, the cloud program goes nowhere. The KMS best practices are a collection of proven options that key management put together, based on a number of successful client engagements in the financial services industry. Use of these best practices will avoid the lengthy and expensive learning exercise, thereby achieving objectives faster and cheaper.

7. **Backup or snapshot standards:** Just as data is backed up in the traditional on-premises world, it has to be backed up for cloud workloads too. The practices and approaches used in the past will not suffice for cloud environments. A cloud standard backup or snapshot uses proven, highly scalable, highly resilient tools and processes that avoid time-consuming, costly, and risky learning exercises and the use of expensive third-party tools, thereby achieving objectives faster with less expense and risk. Cloud-based backup or DR designs for on-premises architectures, while using principles similar to cloud-native environments, will have significantly different implementation architectures. This is because of latency issues, ingress and egress bandwidth, transfer costs and possibly differing data security requirements between on-premises and cloud. Be sure to anticipate these potential differences and make sure they are considered during architecture design and selection.

8. **Virtual networking best practices:** Built in code, and key to an agile framework, virtual networking is the logical isolation of resources via software-defined networks (SDNs). All three major public cloud providers offer SDNs. However, the proven models and software best practices may not be common knowledge within your network engineering group. Developing, testing, and releasing SDN code in the public cloud is often a huge mind shift for IT groups. Best practices are built using software, managed under the strict release processes of software projects, and tested in real time for errors and vulnerabilities. Without this knowledge up front, and built into the project cycle of your cloud before you start, you're running the risk of cloud failure.
9. Monitoring and logging: Monitoring and logging in the cloud offers significantly greater visibility into the operation of your environment. Monitoring takes on a whole new meaning when all infrastructure services are accessible via a common API. Monitoring goes from a reactive service to being in a proactive and preventative position. Monitoring and logging best practices are critical to achieving agility as well as realizing the financial and security benefits of cloud. Each cloud provider has their own cloud watch service; however, they are not equal nor are the processes used to manage them. Without clear visibility into the behaviors of the systems, and knowing what to do—in code—to correct the problems, cloud adoption hits a ceiling of agility.

10. Continuous governance and continuous cost management: The faster you run, the better your control systems have to be. Cloud has flipped the compliance process upside down. It has introduced a new set of variables—new tools, new configuration and approval processes, new job roles, and new rules for companies to follow. The changing environment has turned compliance into a moving target that’s harder to control. Compliance can no longer be managed once or twice a year. In the cloud, compliance needs to be managed continuously. Without continuous protection of your assets against a standard governance framework, the hygiene of the platform drops and costs run out of control. The name of the game is speed of continuous control. It means you need a set of services and practices that are the culmination of industry best practices and are constantly updated to keep your systems healthy.
With proper understanding and planning, your data will be secure in the cloud, if not more so versus on-premises. Actually, your public cloud security can surpass your on-premises security. Considering the paranoia around cloud computing and security, most public cloud-based systems have better thought-out security mechanisms than those in traditional data centers. Because on-premises systems continue to age, hackers can easily defeat their intrinsic security. Moreover, the number of attacks increases weekly, and defenses need to be proactive—more proactive than most enterprise IT organizations are, and likely more proactive than they can each afford to be.

So why have you not gone big with cloud security? Perhaps, it’s just a lack of knowledge about the process to secure your public cloud-based datastore or application. Here are five easy steps to ensure security in your cloud program:

1. **Understand your true requirements:** Many organizations have notions that are not based on reality about legal and compliance issues around the protection of corporate and government data. Things that need to be reviewed in detail include any laws or regulations that require compliance and what technology is mandated. Moreover, existing internal policies around the protection of data must be identified. These should be written down and approved by leadership, so everything is clear and well understood.

2. **Consider identity-based security:** The best approach to cloud-computing security requires that we deal with all assets, including humans, servers, databases, data, processes, services, and others, as identities. These identities can then be managed for access to resources, and as resources themselves. Identities are no longer a part of the infrastructure; they’re part of the application and the data, which means they are firmly in the hands of developers who will need to drive application development along with enterprise security and governance. The most successful and useful cloud security systems are able to manage fine-grained identities to control when and how they interact.
3. **Create a plan:** Many consider security to be one of the things that gets added in the final hours of deployment or migration. The reality is that approaching security in general—and cloud security specifically—requires a master security plan based on the requirements gathered in **Step 1**. Keep in mind, security is systemic in cloud computing. It is a part of every step in the plan. This drives down to the actual solutions, including solution patterns and candidate technology that should be evaluated as a potential fit. Many in IT approach security technology with a bias toward their favorite or existing solutions. Don’t lock yourself into a technology until you’ve understood the requirements and tested the technology.

4. **Select the right security technology:** Make sure your developers have the tools they need to build secure systems, as well as keep your DevOps systems secure. While there are many tools to choose from, security approaches and security technology should be limited to identity-based systems that span most of the systems under management. This is not just about securing DevOps; else, the resulting security solution would still be vulnerable. Once selected, don’t make the same mistake others have by implementing security technologies without ever testing them first. POC testing is mandatory. You should go into deployment with no unanswered questions.

5. **Deploy, test, and monitor:** Deploy the security solution with the understanding that it is not a separate entity from the core system or the data, but is bound to them. Take a few weeks to try white hat penetration testing. This will provide insurance that the solution works, or perhaps, it will point out the need for some additional configuration. Finally, understand that monitoring is required over time.
Three steps to align security and DevOps

What about securing your development pipeline? Let’s get more specific and get into the details of this critical part of your program. You’ll need to reach across the aisle and invite your business counterparts to the table for this discussion. They must be part of the solution as they are key to its success.

1. Standardize on a pipeline

Standardize on a delivery pipeline toolset and bring security in to automate all the different security pieces within it. Identify specific automated places where security can do its check. Once one facet finishes, it moves on to the next portion of the deployment. Often, we see that organizations do not standardize their deployment pipeline and therefore are putting security into the position of maintaining the integrity of many different types of pipelines. Security should become a service provider and treat development as a client. Its mission should be to create a more secure pipeline to help the DevOps team move faster. Development needs to be a source of consistency and security needs to be valued as a point of quality.

2. Do not rejigger the organization—Reallocate tasks

You do not need to replace or reassign people to implement a greater focus on security. Repurposing people’s existing tasks is all you need to do. For example, people who are normally doing just the penetration test of an application might take on additional roles for static app security testing or dynamic applications security testing. When an app is finally released in a waterfall scenario, it gets pen tested. By that time, potentially thousands of lines of code have been written. In a more agile system, those security personnel get the opportunity to shift left in the development lifecycle. Put mechanisms into place to make lighter controls to ensure problems will not exist when code gets released into production.

3. Add new tools

Many organizations do not take on app security. They hope developers write code safely and do pen testing; this is not application security. There are more tools to leverage now, such as SAST, DAST, IAST, RASP, third-party versioning tools, and pre-IDE code checkers. These tools have matured as the space has become bigger. Larger organizations are using them, but they should be employed more widely to help DevOps avoid unnecessary delays in the workflow.
5. How can I unlock continuous innovation once my team is operating in the cloud?

The answer is to go big on DevOps. Many people equate DevOps to IT automation or even CI/CD. Automation and CI/CD are components of DevOps that you will typically incorporate into your DevOps practice but they are not DevOps in and of themselves. DevOps is the progression of the software development lifecycle (SDLC) from Waterfall, to Agile, to Lean. Many legacy processes were derived in the days of biannual releases, which get in the way of progress in the era of Continuous Delivery. To be agile, legacy organizational structures, built to control costs and dictate policy, must give way to new organizational structures that promote high levels of collaboration, transparency, and shared goals. The evolution to DevOps maturity requires a focus on three areas: people, process, and technology.

**DevOps:** A culture shift or a movement that encourages great communication and collaboration to foster building better quality software more quickly with more reliability.

Here are three fundamental actions you must take to enable innovation across your organization once you’ve put in place your cloud program. Remember, just because you built a great racing machine (your cloud platform), it doesn’t mean you have businesses who know how to drive it. The people are critical to your success, and you’ll need to reach out and teach them what you know.

1. **DevOps and people**

Innovation is a much-overlooked area when it comes to transformation. In the days of physical hardware, it was often unfeasible to invest the time and money it took to procure or create new environments to try out experiments or a hypothesis. Many enterprises outlawed experimenting with new technologies without going through a proper vetting process. This mindset often stifled innovation. Employees would experiment at home but could not bring these learnings to work. Stifling innovation often leads to employee turnover because the best and the brightest love to innovate. Cloud changes this, making it easier for engineers to access resources without the rigorous, time-consuming processes.
People skill is another area. Not only do people need to be trained to use the cloud provider’s services, but they must also learn new methods and approaches required to take advantage of the cloud. This includes breaking down department silos to foster greater collaboration between groups that might not have worked together in the past. In the DevOps model, there are many shared responsibilities. Everyone owns security; everyone owns quality—not just the IT people. Specifically, the product owner and the business sponsor also share ownership. When ownership is shared, everyone works toward a common goal.

2. DevOps and processes

One common mistake seen with legacy processes is a lack of analysis of those processes before proceeding with their automation. As a result, enterprises are automating wasteful steps and not realizing the agility benefits they were expecting. If enterprises only implement CI/CD without looking outside the silos and performing a value stream assessment of the complete system, they will only move bottlenecks from the build process to another part of the system and never achieve the desired agility. Engineers must think about the system as a whole, instead of just focusing on automating one component. Unfortunately, system thinking can be a foreign topic to a silo-based organization.

Governance is another important process area. The days of holding multiple weekly review boards for architecture, security, and governance must be put to rest. These processes and mindsets simply do not work in the era of continuous deployment. In this new age, you must trust your automation and institute proactive and continuous monitoring to check for ongoing security and compliance. Manual review by humans just does not scale when multiple teams are able to perform push-button deployments.

3. DevOps and technology

Here, we finally start focusing on IT automation and the famous CI/CD processes. Running systems in the cloud requires new tooling and methods—born-in-the-cloud solutions in the areas of security, monitoring, logging, code repositories, and others. Providing visibility into system health and application state is crucial to providing high SLAs in this new world where deployments happen frequently. Much thought needs to go into building a robust security and monitoring framework that feeds into a central logging solution and can be accessed through a single pane of glass.

The build process should perform security and coding standards scans. Testing should be automated and part of the build process. The build process should produce a score for security, programming standards, and quality. The build should fail if any one of those scores is not at an acceptable level. The goal of this approach is to not let issues progress downstream because it is much more expensive and time consuming to detect problems later in the lifecycle.
Conclusion

Cloud computing is providing enterprises the capabilities to greatly improve their overall agility as an organization. Embracing the cloud to take advantage of this opportunity calls for a complete transformation of an enterprise’s people, processes, and technologies. Remember to communicate the goals and objectives of the project to your team from the onset; to use proven accelerators to realize value sooner; and to promote a DevOps mindset company wide.

Learn more at

hpe.com/cloud