Building the core foundations for Cloud at Scale™

A secure, sustainable and strategic approach for organisations to adopt the public cloud while building a solid foundation for future growth.

amdocs
make it amazing

Table of contents

Cloud at Scale™ in brief

The challenge of adopting Cloud at Scale™

Adopting cloud is complex. Communications service providers are often burdened with complex IT stacks comprising hundreds or even thousands of monolithic, legacy applications.

They must adhere to rigid security and regulatory requirements, while managing vast amounts of personal data. And they face substantial challenges undertaking the organizational and mindset change that a successful cloud adoption program entails. In fact, 80% of first-generation cloud adoption programs failed to meet their goals. Instead of the promised scalability, agility and elasticity, enterprises found themselves with a jungle of siloed, out-of-control migration initiatives, increased costs, little cloud value and even compromised security.

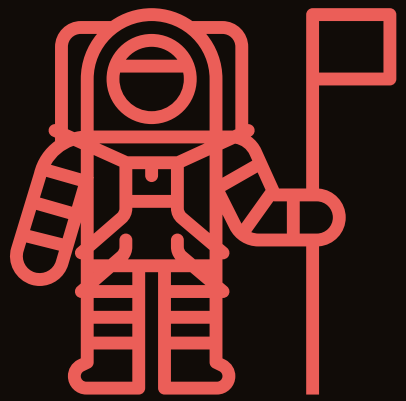
Amdocs "Cloud at Scale™" approach

Sourced, an Amdocs company, diagnosed the causes of these first-generation cloud adoption project failures and developed the Cloud at Scale™ approach explicitly to rectify the errors of Cloud 1.0.

At the heart of the approach is the development of a common, standard, core infrastructure foundation, along with an initial set of pre-defined consumables (templates) that contain the enterprise's security, compliance and deployment opinions. This becomes the foundation on which the entire cloud journey is built, adopting a platform approach to app migration (as opposed to a per app approach) that provides a consistent control plane across all cloud applications within the organization, centralizes common functions such as networking, billing, auditing and security, and launches a migration factory to rapidly migrate hundreds and even thousands of apps to the cloud in a standardized manner.

This whitepaper details the early cloud missteps that caused Cloud 1.0 failures, and recommends best practices for successful adoption of Cloud at Scale™.

The giant leap to cloud... and what might go wrong



The move to the cloud by organisations both large and small is inevitable. The pace of innovation enabled by cloud computing ensures that those who ignore or are slow to adopt it will quickly find themselves disrupted by competitors who can benefit from greater speed to market, business agility, scalability and cost-efficiency.

However, for large enterprises, which are frequently burdened with strict regulatory requirements, adopting the cloud is not a simple exercise. When only taking a tactical and technical approach, enterprises can easily miscalculate the organisational impact of adopting the cloud.

Cloud services can and often are procured with a few clicks of a mouse by individual departments and project teams. However, this can result in numerous challenges when central IT teams lose control of critical infrastructure, along with potentially compromised security and compliance postures. Securely and efficiently taking advantage of all that the cloud offers requires an organization-wide approach, with full support from central IT teams. Small, independent, siloed, and one-off initiatives should be avoided.

While a cloud journey may begin with a single step, even the best organisations can start on the wrong foot when adopting the public cloud. This can lead to false starts, stalled efforts, expensive technical debt, or, even worse, creating security holes exposing sensitive data and vulnerable resources. **Organisations that fail to have a strategy in place find themselves unable to fully realise the benefits of the cloud. Instead, they end up with an inconsistent approach to cloud and incompatible processes struggling to keep up with the pace of innovation.**

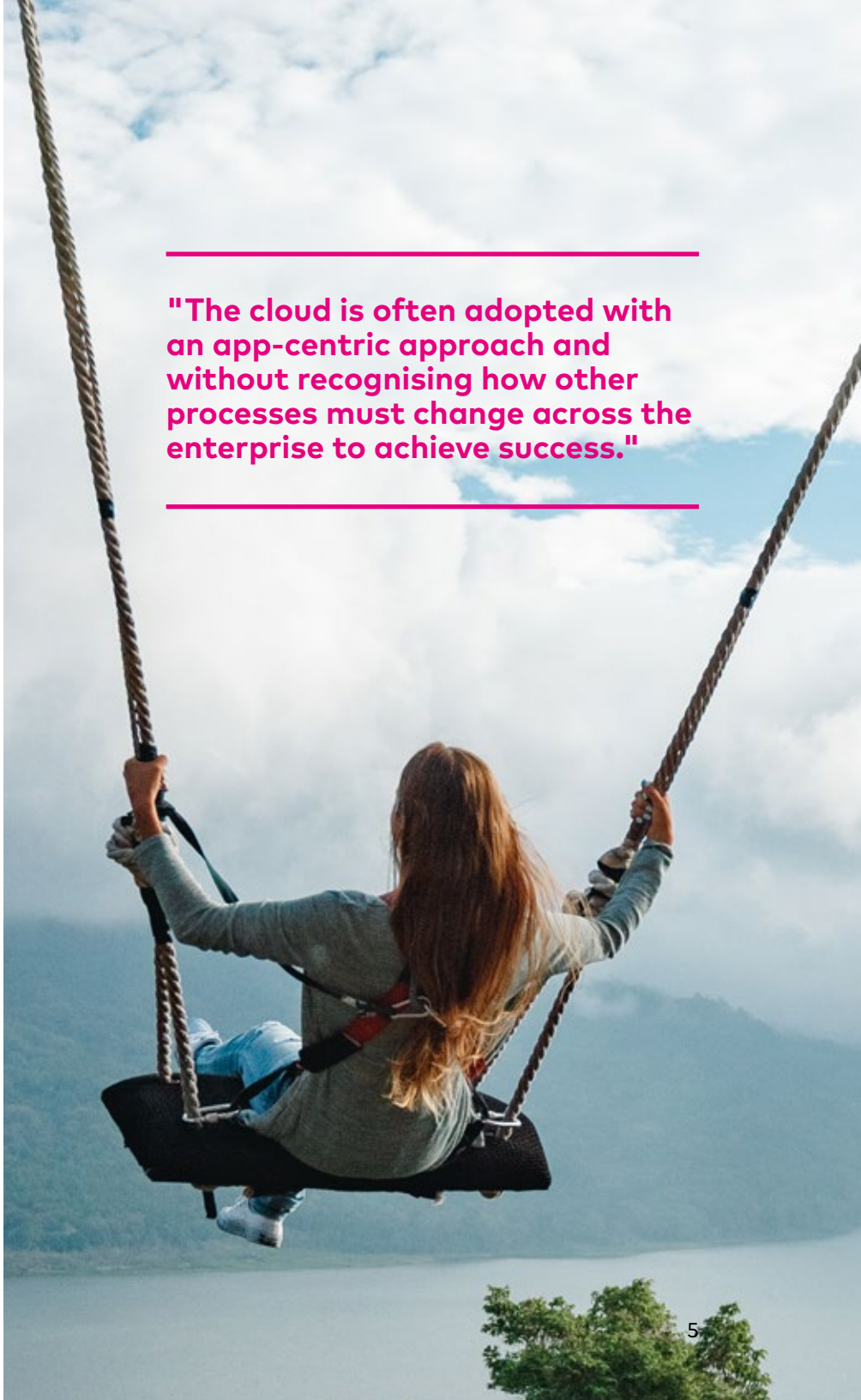
Cloud adoption must be carefully considered, mapped, and aligned to the enterprise as a whole. This paper looks at the dangers of early cloud missteps, best practices for adopting the public cloud, and an approach to starting an enterprise cloud journey that creates a foundation for future success. For organisations that are already using the cloud but find themselves constantly facing blockers and struggling to meet compliance obligations, this paper will provide insights on how to perform a gap analysis to help transform an existing strategy to one that will enable the benefits of the cloud to be fully leveraged in a scalable and compliant manner.

Cloud unchecked: Growing pains and risks

Cloud computing at scale is disruptive in its nature and very different from how traditional IT is typically performed on-premises. To maximise value, a culture and mindset shift must occur throughout the organisation, one that embraces the new model and new approaches to IT infrastructure and application development.

The cloud places all the resources needed to develop, test and launch new applications and services just a few clicks away. But for large enterprises, especially those in highly-regulated industries such as financial services, healthcare and telecommunications, this introduces significant risks. Cloud consumption can quickly spiral out of control, and without proper operational controls and processes, so can security and compliance.

Despite its maturity, there remains confusion across industries around cloud computing, Infrastructure as a Service, Platform as a Service, and how cloud providers such as Amazon Web Services, Microsoft Azure and Google Cloud Platform work. The cloud is often adopted with an app-centric approach and without recognising how other processes must change across the enterprise to achieve success.



"The cloud is often adopted with an app-centric approach and without recognising how other processes must change across the enterprise to achieve success."

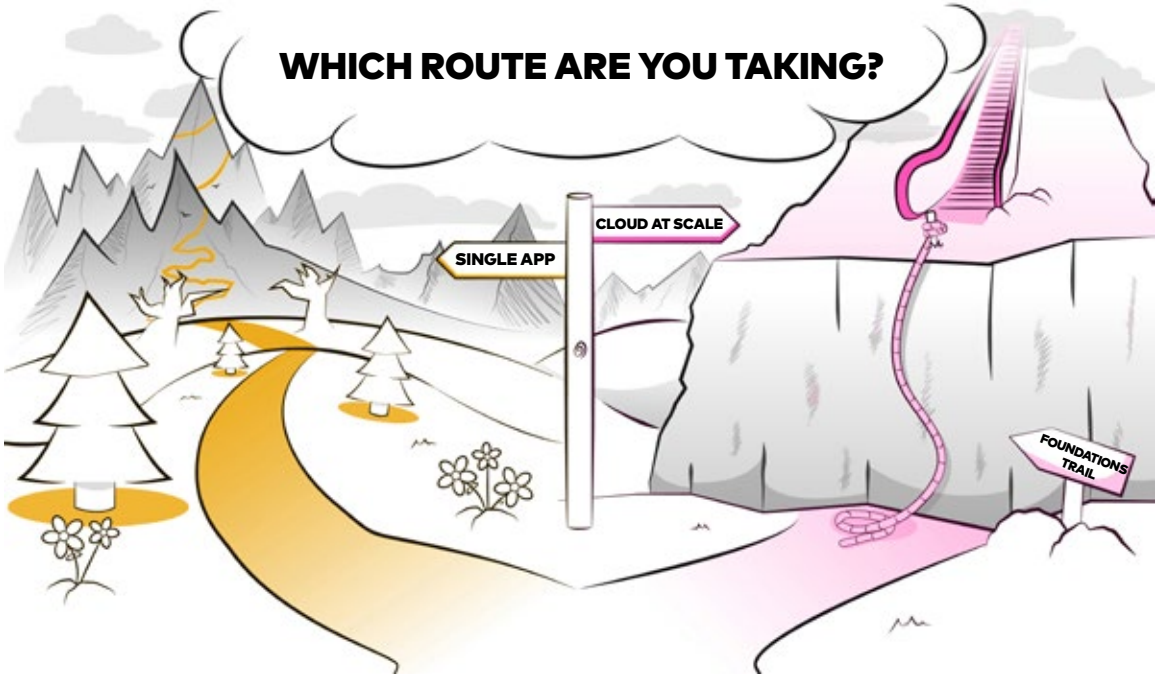


Figure 1. Workload vs platform approach to cloud adoption

In Figure 1, the path on the left focuses on shifting workloads into the cloud on an application by application basis. Typically, this will be driven by the individual business unit responsible for the app, which will take a bespoke approach with limited oversight from a central IT or cloud team.

This results in deployment and operational processes specifically tailored to that particular application. This approach can deliver short-term velocity, and may initially seem like the easier option.

Challenges arise when the next application begins its migration journey, and the organisation finds that the processes established with the first application are poorly suited to this one. As more and more applications are migrated or developed, exemptions and changes spiral out of control. Each application has its own unique set of processes, or the central processes are full of exceptions and patches to make it work for all applications. Either way, migrations and new builds become more complex and harder to deploy, and the inconsistent processes inevitably lead to security holes and auditing issues.

The path on the right uses a central cloud platform approach that provides a consistent control plane across all cloud applications within the organisation, and centralises common functions such as networking, billing, auditing and security. The challenge lies in the initial up-front effort of setting up the necessary team and implementing or building a cloud management platform. The benefits of this approach are scalable, compliant and efficient cloud consumption in the long term. Application teams are empowered to provision cloud resources themselves that are governed by a centralised team, and there is a cloud management strategy in place that ensures compliance, auditability and adherence to best practices.

Challenges in cloud adoption

1. Shadow IT

Shadow or rogue IT is nothing new, but cloud computing makes it easier and often more prominent. The ease at which individual departments and teams can procure cloud resources makes it extremely appealing. However, **operating outside a central IT or cloud team adds complexity and cost and puts the enterprise's security, audit, and compliance posture at risk, especially in highly-regulated industries. In addition, with lines of business acting on their own, it becomes virtually impossible to adopt the cloud in a manner that will scale for the organisation.**

The size and impact of shadow IT are easily underestimated within organisations. It is likely that large enterprises who think they are not currently using cloud services do, in fact, have shadow workloads on one or more public cloud platforms. The security and compliance of such workloads will depend entirely on the experience and capabilities of each respective project team.

The challenge of shadow IT is certainly not exclusive to organisations adopting the cloud without a central team. When a central team is established but is not sufficiently integrated with the application teams, it can result in networking configuration or the availability of services changing according to isolated requirements. Such changes can negatively impact many dependent teams and applications, leading to considerable frustration, and potentially insecure workarounds.

Central cloud, or IT teams responsible for the cloud, should not operate as an island. They need integration and regular communication with application teams and other cloud users, and any significant changes to the platform need to be assessed and discussed before implementation.

2. Mistakes are easily made

Cloud opens the door to tremendous opportunities to innovate. However, if mismanaged, it also opens the door to cybersecurity risks, unexpected costs and other undesirable outcomes. For example, we can create and deploy containers, databases, and storage facilities in seconds and with just a few clicks in the cloud. However, cloud inexperience, default service configurations, or copy-pasting example policies can easily result in publicly accessible resources — leaking company or client data to the Internet. This is bad for any organisation, but is a very costly mistake for heavily-regulated, security-conscious enterprises.

"If IT resources are not deployed strategically in cloud, enterprises soon discover that not all consumption is good consumption."

3. Technical debt

There can be significant value in early cloud adoption in many industries, especially those facing start-up competitors. **However, when this is rushed and unguided by a sound strategy, the initiatives become disconnected from the enterprise's goals, regulatory requirements and business objectives.**

When the organisation makes an inevitable course correction, these technology silos will need to be reworked to adhere to the standards being implemented at an organisation level. Technical debt accrued from acting early without a strategic plan significantly increases costs as security controls and service policies need to be recreated, and applications must be migrated into the new compliant environment. The barrier created by this technical debt results in the organisation spending additional time and budget cleaning up past mistakes rather than building a solid foundation for services and future innovations that drive competitive advantage.

4. Resource consumption

The cloud makes it easy to procure and consume IT resources. However, if these resources are not deployed strategically, enterprises soon discover that not all consumption is good consumption. Suppose 80 per cent of an organisation's applications run on Microsoft SQL Server. In that case, spending time, effort and money moving an Oracle Database server to the cloud might be a great talking point, but it offers low value to the application teams.

Another example is organisations that invest heavily in cloud server capabilities while the application teams are gravitating towards more modern container or serverless architectures. Cloud consumption needs to be assessed for current needs and future targets. The effort, especially in the early days of cloud adoption, needs to focus on those areas of most value to the broader organisation and the majority of applications that will be migrated.

5. Cost inefficiencies

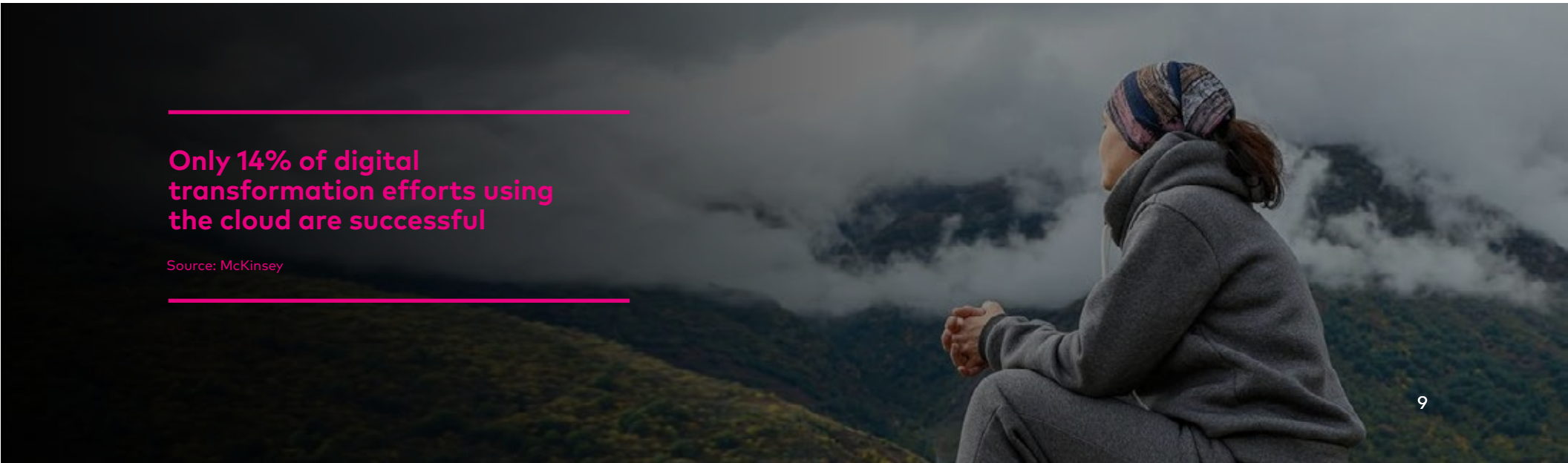
Moving away from traditional data centres into the cloud can bring cost savings by reducing the physical and operational costs and enabling organisations to scale up and down, driven by the real-time needs of workloads. However, organisations might not be maximising these savings because of a lack of understanding of how cloud resources work.

For example, a lift-and-shift of existing workloads into the cloud with no optimisation will rarely lead to significant cost savings compared to on-premises. In some cases, lift-and-shift workloads could even be considerably more expensive in the cloud. **Optimising applications for the cloud by rightsizing servers, using autoscaling, keeping communications within the cloud network, implementing a data and lifecycle strategy, and using managed cloud services where possible, are just some of the actions that can significantly reduce the cloud operational cost.** These are all opinions and guidelines that should be included in any comprehensive cloud management strategy.

6. Process bottlenecks

The cloud can improve application teams' agility and reduce time-to-market for applications, but without an appropriate strategy in place, it will be difficult to capture these benefits, certainly in the long term. Challenges will surface when the organisation scales their cloud consumption by rolling out cloud availability to more teams and by migrating or creating new applications in the cloud.

For example, managers may be overwhelmed by approval processes given the number of cloud services required by applications built for the cloud. While this still holds true for server applications in the cloud, it is exacerbated by modern architectures such as serverless, where the number of distinct cloud service configurations can grow from tens to hundreds for a single application. Application teams may spend more time raising and waiting for change requests than actual application design and development work.



Only 14% of digital transformation efforts using the cloud are successful

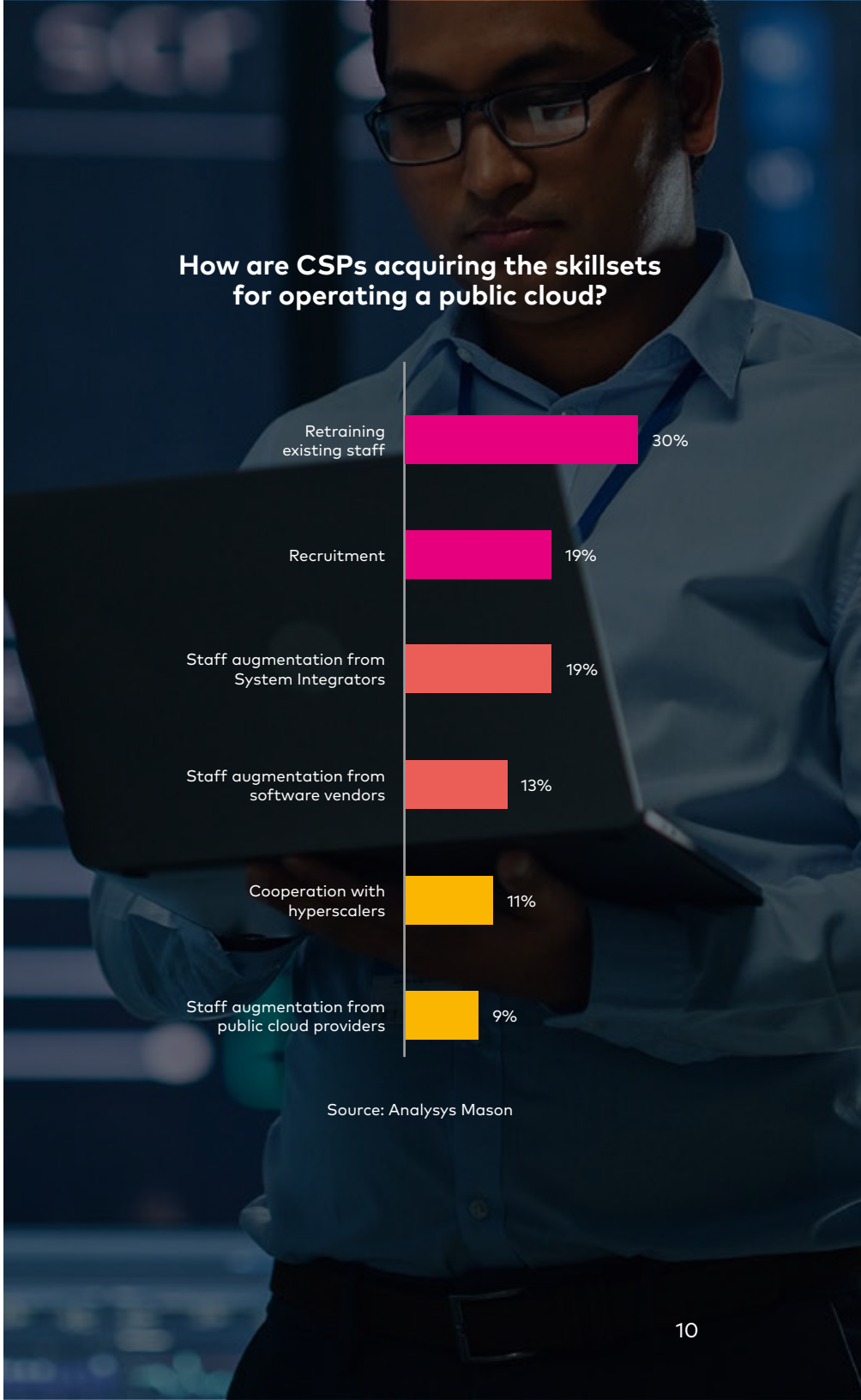
Source: McKinsey

7. Shortage of talent

The shortage of cloud skills in the industry and talent competition with global tech giants make it difficult for organisations to innovate as quickly as they would like. The shortage of talent is worsened if application teams operate their cloud environment in silos. This stifles innovation, creates non-standard approaches for cloud operations, and presents an inconsistent picture to potential candidates.

Organisations often rely on external vendors to augment their cloud, team but soon find themselves limited by the skillsets of inexperienced vendors. This is especially true for regulated enterprises that have specific challenges. Vendors with considerable experience helping SMEs adopt the cloud will often struggle to adapt their existing procedures, templates and architecture examples to work in highly regulated industries. Public best practices established by cloud vendors, consultancies and non-regulated organisations can rarely be used as-is by regulated industries.

Conversely, vendors used to working with regulated enterprises may not have had the opportunity to gain experience with modern architectures such as containerisation and serverless. The proposed approach will often rely heavily on servers, network segmentation and other traditional strategies. However, in doing so, they make it very challenging for the organisation to evolve its use of the cloud with evolving application teams and gain the advantages that more modern approaches can offer.



8. Lack of appetite for innovation

The public cloud is innovating and evolving at a tremendous rate, but an organisation's risk appetite may not match the pace of innovation. For example, organisations that are comfortable with servers in the cloud may be able to adapt to containerisation, but they will take a few years to accept more recent evolutions such as serverless. Depending on the region, such a pace can be due to internal matters and not regulators, who are often more outcome-focused. The pace of change will also be driven by business matters such as competition. In industries seeing considerable competition from smaller, more agile start-ups, the drive to disrupt oneself is significantly higher than in other sectors that are perhaps less subject to such competition due to the high bar or cost to entry.

For organisations willing to embrace change but struggling with keeping up with the pace, the solution, again, lies in a sound cloud strategy. A well-designed strategy is one that can evolve and adapt to support new types of workloads without compromising efficiency and compliance. Automation is a key part of that; the more codified the cloud approach and its applications, the easier and faster it can be modernised and rise to new challenges.

"The more codified the cloud approach and its applications, the easier and faster it can be modernised and rise to new challenges."

Best practices – well begun is half done

Cloud computing has changed the underlying principles of building and running IT applications. To succeed in adopting the public cloud, it's crucial to ensure the fundamentals are in place as early as possible to avoid sprawling technical debt.

It's one thing to migrate a single application to the cloud, but another to achieve organisation- wide cloud adoption, with the ability to scale to meet any demand, improve application velocity and release cadence, avoid bottlenecks and, ultimately, ensure customer satisfaction. For the greatest advantages of the cloud to be fully realised, it must be seen through the lens of how it transforms and impacts the entire enterprise, its people, security posture, governance and compliance requirements.

Based on Sourced's extensive experience helping some of the world's largest and most security-conscious organisations migrate to the cloud, we have established a comprehensive strategy including many best practices for organisations to adopt the public cloud successfully.

Start with a cloud foundation that scales.

To ensure compliance, security, governance, and operational readiness, organisations should build a secure, enterprise-grade platform in the cloud. To enable scalability and compliance, the platform should be managed through automation and achieve equal or higher compliance in the cloud than on-premises, but with security policies modernised to be cloud-optimised.

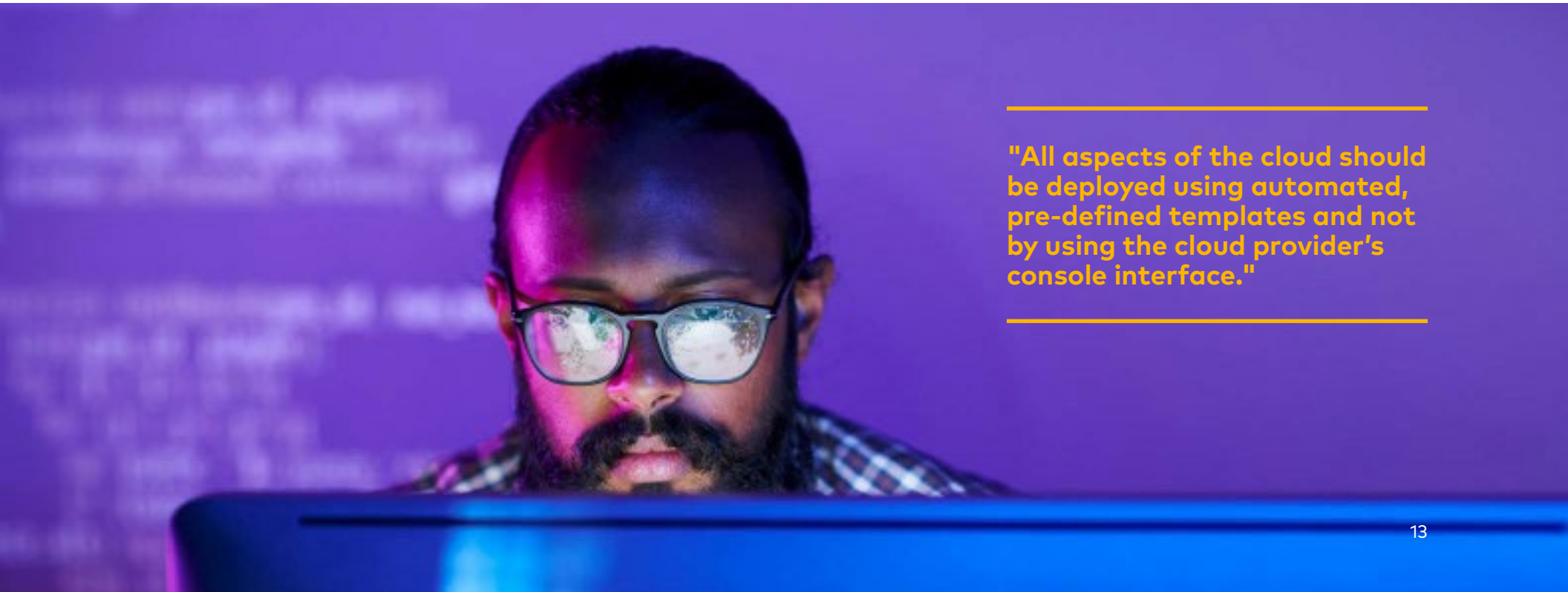
Communication is key here, policies need to be adapted and often evolved for cloud-native architectures, but such changes should never compromise the level of compliance and security required by the organisation or regulators. With an ***everything-as-code*** approach, configuration and maintenance can be automated to eliminate human involvement, errors and unproductive waiting time.

This platform in the cloud becomes the foundation on which the organisation's entire cloud journey is built and thrives — from a single workload to ten, 100 and beyond. However, it must be approached from the beginning with scale in mind, and knowledge and operational capabilities must mature and evolve alongside the cloud platform for the organisation to succeed in this journey.

Adopt a cloud-native, everything-as-code approach

Today, every aspect and layer of IT is becoming software-defined. **Achieving repeatable success in the cloud requires embracing the concept of Infrastructure-as-Code (IaC), which uses templates and machine-readable files to build platform and application infrastructure on demand.** All aspects of the cloud should be deployed using automated, pre-defined templates and not by using the cloud provider's console interface. Such templates can contain, or be evaluated against, the enterprise's security, compliance, and deployment opinions. This eliminates human error and enables the ability to deploy infrastructure quickly, securely and consistently.

This approach also allows the best practices of software development to be applied to infrastructure management. Rather than undertaking a one-off development of an application-specific infrastructure, the enterprise can build a reusable foundation on which to run that application, as well as the next one, and so on. Tools exist to provide automation capabilities and create a Continuous Integration/Continuous Delivery (CI/CD) pipeline to build sustainable infrastructure on-demand that has the security, scalability and consistency needed to accelerate cloud adoption throughout the enterprise. While different lines of business and individual application teams are not permitted to have their own distinct cloud approach, they are enabled to deploy infrastructure and applications themselves within the approach guidelines determined by the central cloud team.



"All aspects of the cloud should be deployed using automated, pre-defined templates and not by using the cloud provider's console interface."

Select the right workload

Selecting the first masthead or lighthouse project for the enterprise's cloud journey is an opportunity to ignite change and inspire buy-in from the broader organisation. The right application will depend on the business DNA of each organisation, but, generally speaking, there are some desirable characteristics to look out for.

- It should be client-impactful. The application should not be trivial but meaningful to the success of the business
- The application should carry both internal and external recognisable branding
- The business plan and proposed architecture should make sense and support the application's perceived migration value
- The application architecture includes cloud-native services
- Ideally, it has a relatively low level of technical and political complexity
- Application and shared services teams must be supportive of the change and have a firm understanding and acceptance of the proposed business plan
- The workload is currently experiencing scale, cost or agility constraints that are tracked in the form of metrics or similar quantified proof
- A before and after comparison can be performed with the available metrics to confirm and highlight the intended migration success
- Migrating the application generates valuable lessons around security, compliance and technology, and reusable Infrastructure-as-Code assets for future projects.

Knowledge gained during this initial stage - and the documentation that will be developed off the back of it, strengthens the foundation that will benefit future applications and drive success in the cloud. This measured, iterative approach to bringing applications to production is key to overcoming the inconsistency challenges of cloud adoption.

Building a Cloud Center of Excellence

A cornerstone of successful cloud adoption lies in establishing a central authority that is responsible for the cloud. A common name given to this team is the Cloud Centre of Excellence (CCoE). The CCoE members are comprised of advocates, high-performers, and forward-thinkers from across the organisation and, if needed, from partners.

They steer the organisation's cloud strategy and associated efforts, maintain momentum, and support and advocate best practices. The team can evaluate suitable workloads for migration and centralise ownership of the cloud while still ensuring different departments have a voice. This helps to ensure an agile, consistent and continuously improving approach that minimises silos and shadow IT risks.

A CCoE can prevent silos from forming, ensure knowledge is shared and application teams are appropriately onboarded, and democratise the operation and management of the cloud environment to greatly improve the chances of long-term success.

When cloud initiatives fail, it is rarely due to the technology. Successful cloud initiatives encompass technology, processes, education, and cultural change within the organisation. There are few IT problems that cloud providers don't already have a service or feature for. **The challenges cloud providers and their services cannot solve are related to people and processes, which is the key focus for the Cloud Centre of Excellence.** They are tasked not only with providing the organisation with the tools to succeed in the cloud but also with showing them ***how*** to succeed in the cloud.

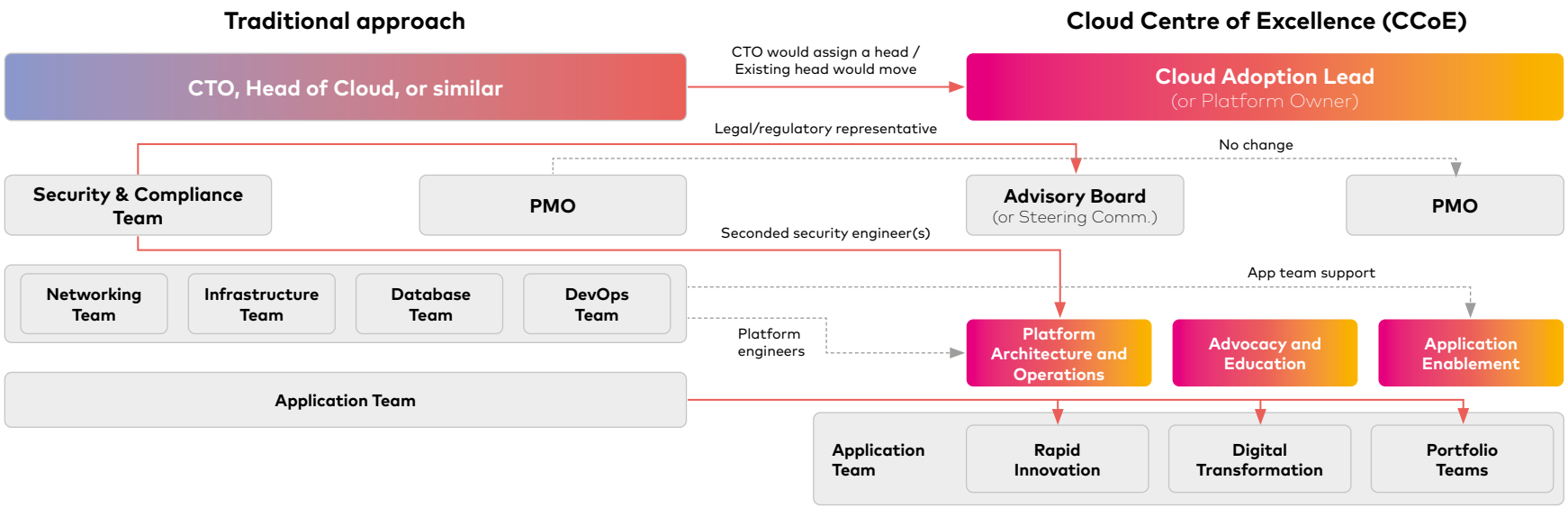


Figure 2. Transitioning from a traditional team structure to a Cloud Centre of Excellence (CCoE)

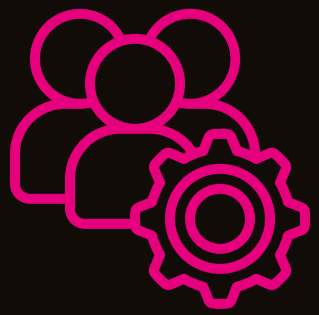
A CCoE team includes members from different backgrounds and expertise. From technology roles to education to operations and support. In Figure 2, we have a common organisational structure on the left. On the right, we present a high-level view of what a CCoE team could look like. The lines show how an organisation might evolve and restructure the traditional teams into a CCoE.

The common structure on the left uses team segmentation to achieve IT security through separation of duties — a common approach to on-premises infrastructure security in large enterprises. In this structure, if the application team needs a new database, the infrastructure team will be responsible for provisioning the server, the networking team for routing the traffic, and the database team for configuring the database and creating the table schema. This works well for on-premises, and it can initially work for servers in the cloud, but it soon becomes a bottleneck as cloud consumption grows and, with it, the appetite for modern cloud-native architectures.

Instead of having separate teams, cloud-native solutions require collaboration across different technical domains such as security, networking, database, DevOps and application development. Working as a single unit helps facilitate resource provisioning and reduces the time to market for applications. Security is managed through fine-grained access policies and centralised controls, rather than via team segregation in a modern cloud environment.

In the CCoE structure on the right, different departments can have a representative on the Advisory board, which helps break down silos and ensure democratic control of the cloud. The ***Platform Architecture and Operations*** team designs, builds, and operates the cloud platform with its automation and controls. The ***Advocacy and Education*** team is responsible for advancing the organisation's knowledge of the cloud. The ***Application Enablement*** team helps individual application teams onboard new applications and use the cloud platform. These are the three pillars of a successful enterprise cloud team.

Enabling and empowering developers



As an organisation scales with the cloud, ownership of resources should shift from infrastructure teams to application teams and developers. However, this is often not the case within organisations — a decision justified by the need for separation of duties to ensure security. A team separate from the application team responsible for provisioning cloud resources presents a blocker, often becomes a bottleneck and is simply not scalable.

We need to enable application teams and developers to be self-sufficient for scalable public cloud adoption. They require the freedom to provision the cloud resources they need for their applications themselves. However, this freedom should not compromise security; we must ensure that the provisioning of cloud resources remains compliant with organisational and regulatory requirements.

Automation over approval gates

The number of services used in cloud-native applications increases considerably. Applications also become less clearly defined, with components splitting into their own scope, and individual components possibly shared across multiple applications. Requiring application teams to request manual approvals for each component and service will lead to a significant volume of support tickets, creating bottlenecks and delays.

Traditionally, application development can require several approvals, from the initial architecture approval to approvals for each environment deployment to specific requests around security, firewalls, internet access and integrations. The delays are exacerbated when multiple approval stakeholders and teams need to be involved and scheduled for each review and approval process.

In the cloud, this approach leads to application teams and developers waiting days or even weeks during the process of getting a single application into production. It is a prime example of applying an on-premises approach to the cloud, completely negating the agility and productivity increases that the cloud can provide. Instead, the organisation needs a cloud-native approach, which is to replace manual actions with trusted, verifiable automation as much as possible.

Cloud controls

Developer enablement with ensured compliance and approval automation can be achieved using rules and automated enforcement of the rules in the cloud. We call these rules and their enforcement controls, and they can be implemented in the cloud account, several cloud services, and the application deployment pipelines.

The latter elevates the importance of such pipelines — they are no longer only a means to get code from point A to point B. **In a modern cloud management strategy, the pipeline provides proof of compliance. It can be ensured that if an application makes it through the pipeline and all its controls without being rejected, then, at least from an infrastructure and permissions perspective, that application can be considered compliant with the organisation's policies.** Pipelines and their controls should also have logging capabilities. As each deployment passes through the pipeline, the controls will log their evaluation of it, providing an auditable trail of compliance proof.

There are four types of controls that we can leverage to ensure sufficient compliance coverage.

Directive controls

Directive controls are guidelines outlining the recommendations and best practices for using the cloud and developing cloud applications within the organisation. Directive controls inform, they do not enforce. So, on their own, they place a high level of trust in the application teams to keep themselves up to date and to follow the directives correctly. Directives are an essential first step in creating controls. They set the rules that the other control types need to guide or enforce in the cloud, and, without documented directives, application teams will not know how to provision compliant infrastructure.

Source: Flexera 2022 State of the Cloud Report N=753

Preventive controls

Preventive controls restrict developers from taking actions that go against the established directives within a cloud environment. For example, preventive controls can be implemented that block the use of specific cloud services or regions that the CCoE does not approve.

Detective controls

Detective controls analyse and monitor infrastructure configuration and changes within the cloud environment for anything not compliant with the directives. Detective controls react after the fact and do not enforce or change anything in the infrastructure. When a violation occurs, a notification will be sent to alert relevant stakeholders, and any follow-up action will be at their discretion.

Corrective controls

Like detective controls, corrective controls monitor the configuration and changes within the cloud environment after the fact to detect any non-compliance. However, when a non-compliant event occurs, it goes beyond notification and can automatically execute appropriate remediation to revert, remove or change the offending infrastructure configuration.

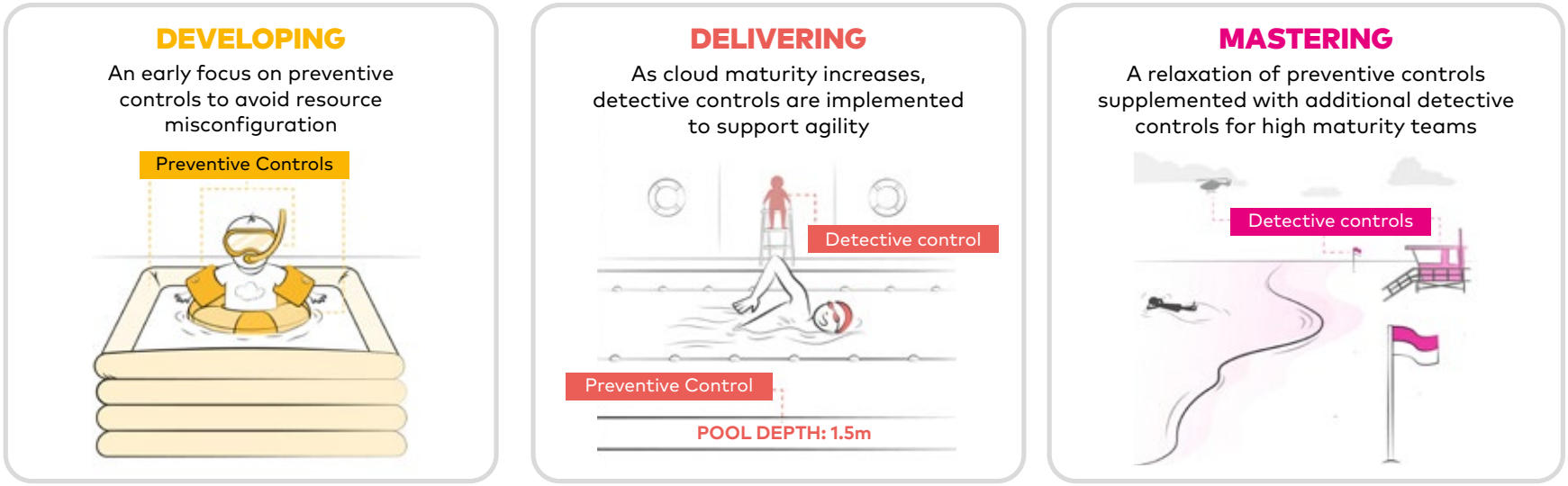


Figure 3. Evolving a controls-based cloud strategy

Cloud controls strategy

We can allow application teams and developers to provision infrastructure themselves through controls. However, the organisation determines exactly which services and which configuration options can be accessed by the developers. This negates the need for some of the manual approvals as compliant infrastructure is ensured by the controls.

Preventive controls are the first line of defence, and best effort should be made to implement as many of the directives as possible in preventive controls — certainly for organisations new to the cloud or with a low appetite for risk. **Preventive controls will stop non-compliance before it can occur, while detective and corrective controls react after the fact.** Preventive controls can be implemented on multiple levels. There are readily available cloud capabilities such as permissions and service allowlists to implement them. Custom controls can be developed that enforce more specific organisational policies.

Detective controls serve two purposes. First, they can catch any non-compliance that circumvents the preventive controls. For example, changes that are made directly in the account by administrators and shadow IT actors. Second, as organisations with a higher tolerance for risk evolve and achieve high maturity in the cloud, they can evolve their cloud strategy and shift from primarily preventive controls to detective — at least in the development environment. This approach places more trust on the developers, giving them the freedom to innovate in the cloud while still tracking any non-compliance.

Corrective controls are used sparingly in practice. The perceived risk of automated rules changing production infrastructure makes it challenging for many organisations to trust them. By the time the organisation has achieved a level of maturity to develop and trust such controls, there may no longer be a need for them. Certainly not if the maturity brings with it a shift in strategy from preventive to detective controls. Corrective controls can still be a good option for data protection. For example, when a datastore is wrongly created with public access, preventive controls can immediately rectify the issue and block access to it. False positives in this situation are justified by the potential risk of an inadvertently exposed data store.

Questions to ask before adopting the cloud

Technology

- What are the implications of rapid business changes on your technology infrastructure?
- How do regulatory compliance requirements influence your technology choices?
- How important is it for your organisation to own the technology infrastructure?
- What changes in customer attitudes and expectations influence your business/IT choices?
- Which technologies and trends are you adopting to support the move to the cloud?

Security and risk

- How can you meet the need for business agility while ensuring security and compliance?
- What are your biggest challenges to meeting compliance standards?
- What do you consider to be the most important elements of a security strategy to reduce the risk in your business?
- What poses the most significant risk to your business: competition, information security, industry disruption or other?
- What measures could the cloud help you take to mitigate that risk?
- How do you envisage your IT infrastructure changing in your planning horizon?
- How do you meet the rapidly changing business demands for new applications and capabilities?
- What are the greatest obstacles to meeting business needs for new application capabilities?
- How can the organisation's current security policies be evolved for the cloud without compromising regulatory compliance?

Strategy

- What are the key motivators driving your company to pursue a cloud strategy?
- What are your executive team's objectives/expectations for your cloud initiatives?
- Who is driving your cloud initiatives?
- Have you performed a gap analysis between your current cloud strategy and the desired state?
- How do you ensure your IT team is connected to the business?
- Which technologies and trends are having the greatest influence on your business strategy?
- How is IT responding as businesses attempt to be more agile to meet today's challenges?

Put your best foot forward with Cloud at Scale™

From day one, the cloud must be viewed as not just a technology solution but one that encompasses people, tools and processes. Sourced's Cloud at Scale™ Core Foundations offering provides the groundwork for this broader, holistic approach. It gives organisations the tools to quickly launch a cloud adoption program based on established best practices. It's designed to achieve early wins while enabling a multi-year Cloud at Scale™ strategy.

The strategy is implemented in our technology accelerators – enterprise-grade platforms for different cloud strategies. Each accelerator is optimised for a particular cloud technology strategy, such as cloud servers, Kubernetes and serverless-first. The accelerators can work together to support multiple technology strategies as required by the CCoE's organisational strategy. Our accelerators are highly customisable and paired with an extensive training programme, enable large enterprises to adopt the cloud quickly while ensuring adherence to best practices and strict regulatory compliance.

The technology platform accelerates cloud adoption by supporting the most common needs while laying the groundwork for further business-specific customisation. In as little as 12 weeks, enterprises can begin adopting the cloud in a compliant manner that avoids the typical risks and missteps — quickly and cost-effectively.

"Our respondents rely on consultants to help them develop the strategy, skills, teams, and processes necessary to take advantage of the public cloud. Just as many look to boutique specialist shops as the big consultancies"

GlobalData
Lessons learned from CSP adoption of public cloud

What we do: The elements of an ideal start

We have a proven, decade-long record of creating low-friction governance and compliance frameworks that address the most challenging enterprise requirements. Our highly-trained consultants and delivery leads draw on that experience to provide the tools, templates and expertise to identify core needs and potential consumption challenges to maximise value through:

1. Consulting services to perform gap and risk analysis and design a comprehensive organisational cloud strategy, including the Cloud Centre of Excellence, education and technology.

2. Integration services to implement and customise the accelerators to the needs of the organisation while teaching how to best leverage the cloud through a cloud-native and everything-as code approach

3. Training and documentation, including a complete user guide to begin building operational capabilities to support and evolve Cloud at Scale ™ going forward, and deep-dive training courses for different types of architecture and best practices.

4. Project delivery services to ensure adherence to schedules and timelines and implement best practices in cloud project management and procedures.

Cloud at Scale™ Core Foundations

The Cloud at Scale ™ Core Foundations platform embraces best practices already in use by Sourced clients across the globe to accelerate cloud adoption at scale, enhance value from the cloud, remove barriers to success, and create early wins. It provides:

Security: Built with the architecture already trusted by some of the largest and most security- conscious organisations in the world

Rapid Time-to-Value: In as little as 12 weeks, start a cloud transformation journey on the right foot with enterprise-grade data centre templates

Low Risk: A short workshop mitigates the risk of throw-away work and ensures an enterprise-grade platform that meets your needs today and for the future

Multi-Strategy: A selection of optimised platform implementations to support different cloud technology strategies, such as traditional server-based workloads, containers and serverless architecture.

Multi-Cloud: Designed to work with different cloud vendors, the platform provides application teams with a consistent cloud experience

Contact us

If you'd like to chat with us about Cloud at Scale, contact Michael Isaacs, Amdocs Global Services at:

Michael.Isaacs@amdocs.com

This white paper was last updated in July 2022 by Thomas Smart.

Amdocs helps those who build the future to make it amazing. With our market-leading portfolio of software products and services, we unlock our customers' innovative potential, empowering them to provide next-generation communication and media experiences for both the individual end user and large enterprise customers. Our 30,000 employees around the globe are here to accelerate service providers' migration to the cloud, enable them to differentiate in the 5G era, and digitalize and automate their operations.

Listed on the NASDAQ Global Select Market, Amdocs had revenue of $4.3 billion in fiscal 2021.

For more information, visit Amdocs at www.amdocs.com

amdocs | make it amazing

www.amdocs.com