Google Cloud

The Google Cloud Adoption Framework

Google Cloud

Table of Contents

Part 1: Executive summary

Part 2: Technical deep-dive

Part 1:

Executive Summary

A unified approach to the cloud

Moving to the cloud offers enormous benefits for businesses. Yet there are risks as well. The challenge is multidimensional, with far-reaching implications not just for the solutions that will run in the cloud, but also for the technologies that support them, the people who need to implement them, and the processes that govern them. The rubric of people, process, and technology is a familiar one. But how do you harness it to move forward?

As one of the earliest organizations to operate entirely in the cloud, Google has been spearheading projects for years that address this very issue — from leadership and people management best practices like re:Work, to engineering-driven software operations methodologies like Site Reliability Engineering, to zero-trust security models like BeyondCorp. It is from work such as this that we've developed a streamlined framework for adopting the cloud.

The Google Cloud Adoption Framework builds a structure on the rubric of people, process, and technology that you can work with, providing a solid assessment of where you are in your journey to the cloud and actionable programs that get you to where you want to be. It's informed by Google's own evolution in the cloud and many years of experience helping customers.

You can use the framework yourself to make an assessment of your organization's readiness for the cloud and what you'll need to do to fill in the gaps and develop new competencies. If you'd like a partner on that journey, we're here for you. We can help you develop a solid strategy and guide you through the process so that you're capitalizing on all that the cloud has to offer, driving the innovation you need to streamline internal operations and scale your brand.

But whether or not we accompany you on the journey, our framework can help you find your way, from your first project all the way to becoming a cloud-first organization. Take it, use it, and move forward to the cloud with confidence.

You can use the framework yourself to make an assessment of your organization's readiness for the cloud

Four themes, three phases

To truly develop a cloud-first organization, there are four realms (we call them themes[1]) you will need to excel in — whatever your business objectives. These four themes define the foundation of cloud readiness:

Learn: The quality and scale of the learning programs you have in place to upskill your technical teams, and your ability to augment your IT staff with experienced partners. Who is engaged? How widespread is that engagement? How concerted is the effort? How effective are the results?

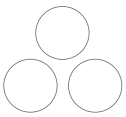
Lead: The extent to which IT teams are supported by a mandate from leadership to migrate to cloud, and the degree to which the teams themselves are cross-functional, collaborative, and self-motivated. How are the teams structured? Have they got executive sponsorship? How are cloud projects budgeted, governed, assessed?

Scale: The extent to which you use cloud-native services that reduce operational overhead and automate manual processes and policies. How are cloud-based services provisioned? How is capacity for workloads allocated? How are application updates managed?

Secure: The capability to protect your services from unauthorized and inappropriate access with a multilayered, identity-centric security model. Dependent also on the advanced maturity of the other three themes. What controls are in place? What technologies used? What strategies govern the whole?

[1] *See Stories versus Themes versus Epics to learn more about agile taxonomy.*

Your readiness for success in the cloud is determined by your current business practices in each of these four themes. For each theme, those practices will fall into one of the following phases:



Tactical: Individual workloads are in place, but no coherent plan encompassing all of them with a strategy for building out to the future.

The focus is on reducing the cost of discrete systems and on getting to the cloud with minimal disruption. The wins are quick, but there is no provision for scale.

Strategic: A broader vision governs individual workloads, which are designed and developed with an eye to future needs and scale.

You have begun to embrace change, and the people and processes portion of the equation are now involved. IT teams are both efficient and effective, increasing the value of harnessing the cloud for your business operations.

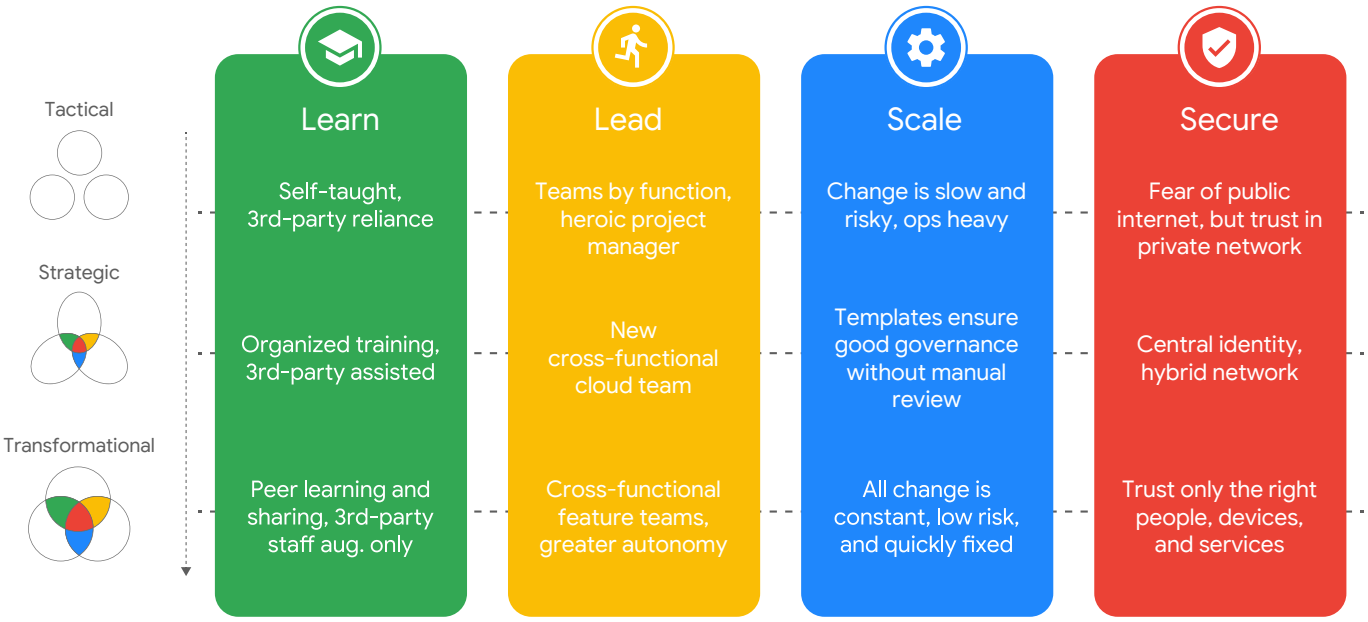
Transformational: With cloud operations functioning smoothly, you've turned your attention to integrating the data and insights garnered from working now in the cloud.

Existing data is transparently shared. New data is collected and analyzed. The predictive and prescriptive analytics of machine learning applied. Your people and processes are being transformed, which further supports the technological changes. IT is no longer a cost center, but has become instead a partner to the business.

In the tactical phase, you are reducing costs with a quick return on investment and little disruption to your IT organization. This is a short-term goal. In the strategic phase, you increase the value delivered by your IT organization by streamlining operations to be both more efficient and more effective. This is a mid-term goal. In the transformational phase, your IT organization becomes an engine of innovation, making it a partner to the business. This is a long-term goal.

The Cloud Maturity Scale

When you evaluate the four themes in terms of the three phases, you get the Cloud Maturity Scale.



In each of the themes, you can see what happens when you move from adopting new technologies ad hoc, to working with them more and more strategically across the organization — which naturally means deeper, more comprehensive, and more consistent training for your people, which in turn means streamlined and updated processes, which in its turn drives innovation. The whole organization gradually transforms.

When you are fully invested in the cloud, fully harnessing its capabilities, you are then a cloud-first organization.

Fine-tuning your direction with epics

Once you've determined where you are in your cloud maturity journey, it's time to move forward. To scope and structure your program of cloud adoption, you will implement a number of workstreams (which we call epics[2]). The epics are defined so that they do not overlap, they are aligned to manageable groups of stakeholders, and they can be further broken down into individual user stories, making your program planning easier.

Here's a look at those epics within the familiar rubric of people, technology, and process. If you can do only a subset of the epics, focus on the ones in the colored segments. Those are the epics that align with Learn, Lead, Scale, and Secure; and so those are the epics that will define your journey to successful cloud adoption.

[2] *See Stories versus Themes versus Epics to learn more about agile taxonomy.*

The Google Cloud Adoption Framework

And those are the three components of the framework Google Cloud uses to guide customers seamlessly to the cloud: the **three maturity phases** applied to the four **cloud adoption themes**, and the **epics**. With the Cloud Maturity Scale, you determine where you are in your journey to the cloud. With the epics, you devise a way to get to where you'd like to be. You can use the maturity scale and the epics with any cloud provider, of course: the framework is technology agnostic. But if you'd like to ensure success, you might consider engaging Google Cloud to be your guide.

Working with a Technical Account Manager (TAM), you can perform a high-level assessment of your organization's cloud maturity, which will tell you how to prioritize your training and change management programs, your partner relationships, your cloud operating model, and your secure account configuration.

The Adoption Framework streamlines your journey to successfully adopting the cloud. Working within the framework, a TAM can guide you along that journey, from your first cloud project to becoming a fully cloud-first organization.

Getting started

The details in the technical deep-dive spell out the foundation for moving forward, but at a high level, the process looks like this.

Assess your current cloud maturity

Introduce your stakeholders to the four cloud adoption themes, that is, to your team's ability to continuously **learn,** effectively **lead,** efficiently **scale,** and comprehensively **secure** in the cloud. Use the summary tables provided for each theme in the technical deep-dive as a reference for discussion. Consider assessing all attributes in the form of a survey for stakeholders to fill out.

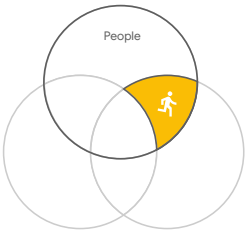
Ask yourself how far you want to go

Discuss within your team which stage of cloud maturity your business should aim for. Chances are that, to begin with, stakeholders across different levels of your IT organization will not be aligned and that they'll point out that the incentives vs. risks don't yet match their aspirations. Consider focusing on tactical objectives in the near term to serve as a stepping stone for later strategic or long-term transformational objectives.

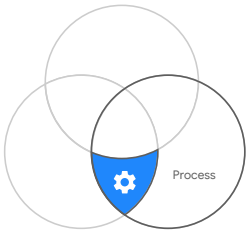
Plan your cloud adoption program

Take action on any cloud adoption epic for which you've identified a gap and pay particular attention to the epics that live inside the cloud adoption themes. Keep in mind that your actions are a means to one of four ends: developing a training program, devising your change management program, designing your cloud operating model, or securely setting up your Google Cloud Platform (GCP) account.

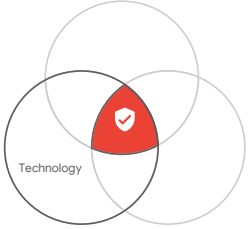
Training Program



Change Management Program



Cloud Operating Model



Secure Account Setup

Find the right workloads

Even the greatest degree of cloud maturity is inconsequential without critical workloads in production in the cloud. Start with simple, non-business-critical applications to develop the muscles and confidence in your cloud competencies. As you develop your organization's abilities to learn, to lead, to scale, and to secure, you should also be ready to tackle more complex and critical applications in lockstep.

Should you begin with workloads? Or with a cloud operating model? A startup company may have a bias toward action, putting workloads into production quickly and assuming greater operational risk in return. An enterprise with a top-down cloud adoption approach may prefer to first invest in a cloud operating model and playbooks before any workloads are deployed in the cloud.

Which workloads and when are up to you.

As you develop your organization's abilities to learn, to lead, to scale, and to secure, you should also be ready to tackle more complex and critical applica-tions in lockstep

Part 2:

Technical deep-dive

Google Cloud

Introduction

The move to the cloud can be arduous — unless you plan well from the beginning.

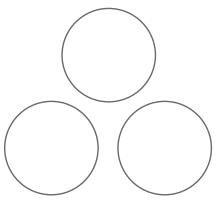
The Adoption Framework helps you with that planning. The framework comprises the Cloud Maturity Scale, which enables you to analyze where you are now in your journey to the cloud, and the epics, which help you organize how you will get to where you'd like to be.

The Cloud Maturity Scale measures your organization's readiness for the cloud by considering your current business practices (which it classifies into one of three phases) across four themes. The epics chunk the actions you will need to take into discrete, and discretely measurable, workloads that map to the same four themes.

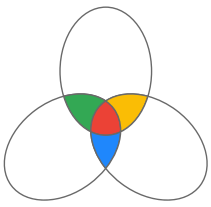
The Adoption Framework is derived from Google's experience of helping hundreds of customers make their way to the cloud. By working within the framework, you can ensure that you are making the right choices, both now for current workloads and with an eye to the future, so that the investments you make today continue to serve you well as you move more and more operations to the cloud. By working within the framework, in other words, you make the most of your resources from that first workload on.

The cloud maturity phases

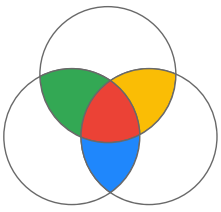
The Cloud Maturity Scale is based upon the three phases of cloud maturity, as they apply to the cloud adoption capabilities (that is, the themes) you will need to master. These three phases apply to any business's journey to the cloud, and they are defined by the business practices current at the time:



Tactical



Strategic



Transformational

Businesses that make the most of the cloud — businesses that use the cloud to drive innovation — are businesses that work towards the transformational phase, which is a long-term goal. But you will achieve short-term successes at the tactical and mid-term successes at the strategic phases as well, and in fact each of those two phases is necessary and useful.

Looking more closely at those phases makes clearer the benefits of each, and the way that one phase prepares the way for the next.

Tactical maturity

Tactical cloud adoption can achieve the short-term business objective of **optimizing cost** within your existing IT solutions, for example, by optimizing heavily underutilized compute and storage resources or by removing the operational overhead and delay of manually procuring and provisioning resources.

As an organization with tactical cloud objectives, you look to execute projects with minimal change to your IT teams (people), your applications and software tools (technology), and your operating model (process). This is an important phase in the journey to making the most of the cloud, and it should not be undervalued.

As an organization with tactical cloud objectives, you look to execute projects with minimal change

The benefits of a tactical degree of cloud maturity are contingent on the outcome of your total cost of ownership (TCO) analysis[3]. Should you anticipate only marginal cost benefits from this approach, you may regard your cloud adoption merely as a lateral move and be tempted to aim straight for the strategic phase. Be cautious of making this leap if your business does not already have firsthand experience running production use cases in the cloud today. Just as there is a cost to moving to cloud, there is also great value in the lessons learned through experimentation. The tactical phase lays the foundation for the work you will do in the strategic phase.

[3] *As discussed in McKinsey: Cloud adoption to accelerate IT modernization and True Cloud Justification: Moving Beyond TCO Savings.*

Strategic maturity

A strategic degree of cloud maturity is sufficient to achieve the mid-term business objective of **increasing value** delivered by your IT organization. This level is achieved by noticeably improving the efficacy and efficiency with which IT teams develop and operate software solutions, as well as by modernizing the architectures of those solutions to take advantage of cloud-native services and platforms.

As an organization with strategic cloud objectives, you will likely implement some degree of change to your IT teams (people), your applications and software tools (technology), and your operating model (process). This change can be limited to an isolated part of your IT organization and still be effective, providing a blueprint and early success stories that can be expanded when the IT organization is ready for comprehensive, transformational change.

A strategic degree of cloud maturity achieves the mid-term business objective of increasing value delivered by your IT organization

Transformational maturity

A transformational degree of cloud maturity is necessary to achieve the long-term business objective of reforming your IT into a sustainable **engine of innovation** that powers your business transformation. Rather than a cost center, IT is now a partner to the business.

An innovation center's key contribution to the business is the data and insights derived from the transparent and thoughtful sharing of existing data, the collection and analysis of new data (for example, sentiment, image, voice), and the application of predictive and prescriptive analytics (machine learning). You should also apply this data-driven approach to your IT organization itself, iterating on new features in a truly agile fashion, accelerating the speed at which you can deliver innovation.

As an organization with transformational cloud objectives, you face the prospect of comprehensively reorganizing your IT organization. Concretely, this means facilitating greater lateral awareness and knowledge exchange and empowering individual contributors or project teams to make more decisions

As an organization with transformational cloud objectives, you face the prospect of comprehensively reorganizing your IT

autonomously, measured against agreed-upon service-level objectives (SLOs). You take a cloud-first position, in which cloud-based services and best practices are the new norm. To support that, you reward experimentation and individual initiative, even in the event of failure, and understand how to reasonably price the value of what is being learned against the cost incurred by your cloud hosting bill.

The Cloud Maturity Scale

Bringing the three phases of cloud maturity to bear on the four themes of cloud adoption results in the Cloud Maturity Scale, a powerful tool for assessing where you are in your journey to the cloud. It does this by measuring your current practices against the known foundations for success. If you make the investment into these foundations from the start, you will be supporting your organization's ability to support increasingly ambitious business objectives, complex software solutions, and cloud-native architectures.

If you make the investment into these foundations from the start, you will be supporting your organization's ability to support increasingly ambitious business objectives

In other words, you will be supporting your organization's journey to transformational cloud maturity. At this phase, your organization will have mastered the ability to continuously **learn**, to effectively **lead**, to efficiently **scale**, and to comprehensively **secure**.

Getting to that point involves planning and successes at the two phases preceding. To ensure you're focusing your efforts on the most impactful areas, you'll want to understand the four themes in depth, with attributes illustrating how each evolves over time across the tactical, strategic, and transformational phases.

Learn

Cloud Adoption Epics: Upskilling, External Experience

Your organization's ability to continuously learn is determined by your efforts to upskill your IT staff while also taking advantage of the experiences shared by third-party contractors and partners. This two-pronged approach ensures that you apply cloud computing best practices idiomatically to Google Cloud Platform (or any other public cloud provider), tailored to your business needs and without having to climb the steep learning curve of doing things for the first time.

Your staff will be more familiar with your organization's unique idiosyncrasies and understand its technical and cultural nuances, while supporting third parties will have the experience of having completed multiple prior cloud migrations across a broad spectrum of customer solutions.

TACTICAL	STRATEGIC	TRANSFORMATIONAL
Self-motivated and isolated upskilling only, using sources like online docs and YouTube. Third parties cover for general knowledge gaps and have admin access to the entire GCP account.	Training classes and certifications offered to anyone interested. Hiring for new cloud-related roles. Third parties provide specialist knowledge and have break-glass admin access.	Peer-to-peer culture of continuous learning through wikis, tech talks, hackathons. Updated roles and responsibilities for entire IT staff. Third parties serve as staff augmentation only, without privileged access.

Tactical maturity

Upskilling is on a best-effort basis, reliant on individual self-motivation and free educational resources like online documentation and YouTube.

Third-party contractors and partners are relied upon to deliver essential work required to achieve the objectives set out by the business. They typically enjoy wide-ranging and ongoing privileged access to your organization's cloud estate and serve as a first point of escalation in the event of a technical question or an operational incident.

You expect to be able to achieve tactical objectives with the IT staff you have and are not taking action to hire new staff with prior cloud experience.

Strategic maturity

Upskilling is program managed and offered to any IT role who is directly or indirectly responsible for contributing to a successful cloud adoption. A learning plan has been published, training classes (online or offline) are offered on a regular basis, and achieving formal certification is encouraged and budgeted for.

Third-party contractors and partners provide subject matter expertise to fill the IT staff's remaining knowledge gaps or where the topic is so narrow and deep that it would be unreasonable to expect your IT staff to upskill to that level. These external parties serve as a second-tier point of escalation in the event of a technical question or operational incident that cannot be answered or resolved internally within your IT staff. As such, they will typically have moderated access to the organization's cloud estate and be authorized (and audited) to escalate their privileges in break-glass scenarios that require quick and determined intervention.

You are actively opening new roles and are hiring for people with prior cloud experience to complement the IT staff as it upskills itself on cloud computing best practices.

Supporting third parties will have the experience of having completed multiple prior cloud migrations across a broad spectrum of customer solutions

Each IT staff member is given a GCP sandbox project and a limited budget for them to experiment with and test new ideas.

Transformational maturity

Upskilling is continuous and collaborative. In addition to a regular formal training program, IT teams and individual contributors host regular hackathons and tech talks to maximize knowledge sharing. Going one step further, IT staff are encouraged to demonstrate thought leadership to the industry through public blog articles and public speaking. This outreach serves a double function of challenging staff to stretch themselves and also to attract new talent to be hired.

You have reviewed and, where needed, redefined all roles and responsibilities to reflect the new requirements of a cloud-first IT organization.

Third-party contractors and partners serve primarily as staff augmentation with no privileged access and very few areas of exclusive knowledge. Most technical questions can be answered internally, and all incident response playbooks can be executed entirely in-house.

Lead

Cloud Adoption Epics: Sponsorship, Teamwork

The effectiveness of your organization's cloud adoption is determined by the visibility and value of the mandate issued top-down from your sponsors (which include C-level executives as well as middle management and team leaders) and the motivational momentum generated bottom-up from your teams' cross-functional collaboration. These two counterparts together are responsible for clearly articulating objectives, making informed decisions, and executing them in concert with multiple functions.

Sponsors control which resources are allocated to your organization's cloud adoption efforts and bring stakeholders from different business functions and reporting lines together. However, they must ultimately rely on an agile and cross-functional group of cloud early adopters to practically implement their strategy.

TACTICAL	STRATEGIC	TRANSFORMATIONAL
Cloud adoption driven by individual contributors within one project team. Collaboration with other parts of the IT org is difficult. Endorsement from senior management. No extra budget	Cloud adoption is driven by a small cross-functional group of advocates, working across project boundaries. Collaboration outside this group is difficult. Endorsement and extra budget by C-level	Autonomous product development teams. Error budgets and blameless postmortems are recognized at the C-level. Org-wide regular progress updates.

Tactical maturity

Sponsorship is limited to senior management from or for one line of business. Their primary contribution is delivering the mandate ("signing off") and passing it down their reporting line to be executed upon. Sponsors only get actively involved as a final point of escalation when progress is otherwise hampered.

Cloud adoption progress is driven by individual contributors with a personal interest in cloud computing for their solution(s). The ability for early adopters to collaborate with other IT roles is subject to the friction of the incumbent org structure and reporting lines.

Because the scope is limited to the project or line of business that this team of early adopters is aligned with — and must operate within that budget — their output will not be embedded with central IT. Depending on the perspective, the outcome is either a "minimum viable cloud" or "cloud shadow IT."

Strategic maturity

Sponsorship extends up to the C-level. Each manager in the reporting line has clearly defined objectives and KPIs that support the organization's cloud adoption. Sponsors' key contributions include actively reaching out horizontally to other IT or business functions to clear the critical path of roadblocks and visibly and continuously championing the journey.

Performance indicators prioritize traditional IT service-level objectives over the speed of experimentation, innovation, and recovery from failure.

Cloud adoption progress is driven by a dedicated cross-functional team (Center of Excellence) of advocates, working across project boundaries. All critical IT roles inside this COE are filled, for example, application architect, software or data engineer, networking engineer, and identity/directory admin, across operations, information security, and finance. Team members are committed full-time or part-time, and their job title and their personal performance indicators are updated to reflect their new responsibilities.

Sponsors must ultimately rely on an agile and cross-functional group of cloud early adopters to practically implement their strategy

Cloud adoption may also be complemented by a dedicated technical project manager who is familiar with the IT organization, the stakeholders, and the technology landscape.

Transformational maturity

Sponsorship is comprehensive across the entire C-level to include marketing, finance, operations, HR, and more, and extends down to all levels of management. They comprehensively and consistently set the tone for a culture of experimentation and innovation within teams. Error budgets for software services are accepted and understood at the highest level (CEO), and a culture of blameless postmortems is fostered throughout the IT organization.

Project teams operate in an environment of transparency and open information sharing and enjoy enough decision-making autonomy to be able to experiment ad hoc without having to ask for permission or having to wait for resources to be provisioned. (Data governance and cost control are now a function of automation, not manual managerial process.) Failures are celebrated for the valuable lessons that the team has learned and will be shared with the wider business for posterity. An individual's mistake is interpreted as a collective or systematic failure that must be addressed as a whole, not by reprimanding the individual.

Scale

Cloud Adoption Epics: Architecture, Continuous Integration and Delivery (CI/CD), Infrastructure as Code

Your organization's ability to scale in the cloud is determined by the extent to which you abstract away your infrastructure with managed and serverless cloud services, as well as the quality of your CI/CD process chain and the programmable infrastructure code that runs through it.

Because everything is managed via an API, automation can pay greater dividends in the cloud than in any other environment. Not only does it reduce human toil and serve as automatic documentation, it is also instrumental in making change low risk and frequent -- the key ingredient for innovation.

TACTICAL	STRATEGIC	TRANSFORMATIONAL
All cloud resources are provisioned manually. Solutions run in long-lived VMs, and OS must be maintained. Changes are reviewed manually, are high risk, and are deployed infrequently and manually.	Project foundations are provisioned from templates. Solutions run in immutable VMs or containers, and access is locked down. Changes are tested automatically, are medium risk, and are deployed manually.	All cloud resources can be (re)created at the push of a button, within minutes. Solutions embrace serverless cloud services. Changes are constant, are low risk, and are deployed with a programmatic strategy.

Tactical maturity

Use of managed or serverless cloud services is limited. Instead, a continued reliance on self-managed, long-lived virtual machines (VMs) provides a familiar computing platform at the risk of entropy ("config drift"), making consistent and secure operations increasingly hard over time. Because there is more to be managed, there is also more to be measured, increasing the burden of collecting quality, high-frequency events and metrics.

Changes to application code and environment configuration are reviewed and controlled manually, for example, by a change advisory board. They are often considered high risk and deployed infrequently, measured in weeks or even months.

The provisioning of cloud resources is performed manually via the GCP Web Console or command-line interface (CLI). Infrastructure automation tools like Deployment Manager or Hashicorp's Terraform [4] are not leveraged. While the use of the GCP Web Console or CLI is already a great improvement over the manual process of racking and stacking servers, it only marks the beginning of the cloud's potential for automation.

Strategic maturity

VMs are designed to be immutable, thereby greatly reducing the scope for change to a system. Environment configuration is baked into versioned VM images, and stateful and stateless workloads are cleanly separated to allow for elastic horizontal scaling. Inside the VM, configuration values and keys are stored only in-memory, and outside the VM only in discrete services like the GCP metadata service, Cloud Key Management Service, or Hashicorp Vault.

The risk of change is considered to be mostly moderate. Deployments to production environments are executed programmatically, but triggered manually, and can be easily rolled back if necessary.

Because everything is managed via an API, automation can pay greater dividends in the cloud

[4] *https://www.terraform.io*

Application teams go beyond basic monitoring and logging, making use of application performance monitoring (APM), either through Stackdriver or through a third-party solution to deliver near real-time insights into service health under real production loads, 24/7.

The provisioning of GCP projects includes all associated configurations (like VPC networking, billing account, and Cloud Identity and Access Management policies) and is performed programmatically via Deployment Manager or Hashicorp Terraform, based on a limited set of inputs like cost center, data sensitivity, team ownership, and dependency with services hosted in other GCP projects.

Transformational maturity

Production VMs allow shell access in break-glass scenarios for debugging purposes only. Self-managed services are replaced with managed equivalents (for example, Cloud SQL, Cloud Memorystore) or server-less/SaaS alternatives, where feasible, to minimize the operations overhead of IaaS-based services.

The risk of change is considered to be low. Deployments to production environments are executed programmatically and automatically, using phased strategies (canary, blue/green, and so on).

Logging and monitoring are comprehensive and cover every service-level indicator that underpins each service-level objective.

All cloud resources are provisioned programmatically via Deployment Manager, Hashicorp Terraform, or directly via GCP's RESTful APIs. Entire production environments can be (re)created within minutes in another zone or region.

Secure

Cloud Adoption Epics: Access Management, Data Management, Identity Management

In the narrow sense, the security of your cloud estate is determined by your ability to guarantee who may perform which action on which resource (identity and access management) and your understanding of the data that needs protecting, ensuring it is appropriately catalogued, encrypted, and guarded from exfiltration, to name just a few considerations.

In the more holistic sense, your security posture relies on the advanced maturity of the other three cloud adoption themes: 1) continuous learning of the latest technical vulnerabilities and security best practices, 2) leading by setting measurable security objectives and rewarding a culture of blameless postmortems, 3) scaling through automation which, in turn, minimizes human error and maximizes auditability.

Because security is so essential and because it cuts across all dimensions and themes, it lives at the very center of the cloud adoption model.

TACTICAL	STRATEGIC	TRANSFORMATIONAL
Staff identities provided solely by Google.	Staff identities are synced from corporate directory.	All service-to-service communication is authenticated and authorized.
Overreliance on primitive IAM roles (owner, editor, viewer).	Predefined IAM roles follow principle of least privilege.	IAM policies are continuously monitored and corrected.
Strong reliance on perimeter security and implicit trust inside private network.	Hybrid security model, relying on both network and application layer.	Multiple layers of network security, from internet to VPC subnet.

Tactical maturity

User identities manifest themselves as Google Cloud Identity[5] accounts under an organization domain name, and all consumer accounts for Google Analytics, Adwords, Play, YouTube, etc. are now under the control of the enterprise. These identities are not yet synchronized with the organization's central identity solution, e.g., Microsoft Active Directory, and therefore not governed by a single source of truth.

Cloud IAM policies predominantly rely on the convenience of project-level Primitive Roles (Owner, Editor, Viewer) rather than following the principle of least privilege. Default permissions allow for any user to create GCP projects and billing accounts. Cloud IAM permissions are not continuously monitored with tools like Forseti Security[6], and the GCP Admin Activity and Data Access logs are not systematically audited. Service accounts can be created freely, and private keys for service accounts are not automatically rotated.

An overreliance is placed on the network to establish a secure logical perimeter around all hosted data and applications: firewalls are used as a critical component to restrict access based on contextual information like the IP address of the client or the port of the application. Communication between clouds and data centers is encrypted using virtual private network (VPN) tunnels by default, with little regard to the efficacy of inter-application encryption using Transport Layer Security (TLS). VPC Service Controls are enforced around fully managed GCP services like Cloud Storage and BigQuery as a matter of principled policy, rather than based on the sensitivity of the data.

Strategic maturity

User identities are synchronized to Google Cloud Identity from a directory service like Active Directory or OpenLDAP, thereby maintaining a single source of truth and a simpler governance model.

Because security is so essential and because it cuts across all dimensions and themes, it lives at the very center of the cloud adoption model

[5] G Suite accounts are Cloud Identity accounts with an associated G Suite user license.
[6] https://www.forsetisecurity.org

Users are authenticated either with the same synchronized password or via a third-party single sign-on (SSO) service. 100% of all user accounts use two-step verification (e.g., SMS or code generator app) to defend against phishing attacks, albeit not with a hardware security key.

Cloud IAM policies reference a much more granular set of predefined roles, rather than the coarse primitive roles. The Project Creator and Billing Account Creator roles have been removed from the organization level to ensure a basic degree of cloud resource governance.

The network-based security perimeter (VPC) is augmented by additional security layers that protect individual services, for example, via Google's global Cloud Load Balancing with TLS configured, Cloud Identity-Aware Proxy, and Cloud Armor. This, in turn, lowers the risk profile of exposing a private service to the public internet.

Transformational maturity

All service-to-service communication is authenticated and authorized. Little trust is placed in the circumstance that they might share the same virtual private cloud (VPC) and/or VPN. For that same reason, internal firewall rules don't allow for specific IP addresses or ranges but rather for specific service accounts.

A comprehensive understanding of the contents of all your data stores provides the threat profiles for which you can design your security and data governance models, considering scenarios of both unauthorized and inappropriate access.

100% of all user accounts use a hardware security key[7] as their second factor to effectively defend against phishing attacks. SMS and code generator apps are understood to be insufficiently safe.

GCP Admin Activity and Data Access logs are regularly audited through Stackdriver and automatic alerts have been configured to watch for patterns that match your threat profile. Cloud IAM permissions and firewall rules are continuously monitored and corrected with tools like Forseti Security.

[7] *https://cloud.google.com/security-key/*

The epics

Once you've assessed your cloud maturity, you're ready to translate those insights into actionable programs of work. That's where the epics come in: clearly defined, nonoverlapping workstreams tied back to the four themes and aligned to your stakeholders. The epics situate the work you will be doing within the familiar rubric of people/process/technology. With the epics, you will design programs to help you solidify your maturity in any given phase, or take it to the next level.

For a lean approach, focus on the epics inside the four cloud adoption themes. For an enterprise-grade approach, you will likely want to explore all epics together.

Access management

Objective: ensuring that only the right people and services are authorized to perform the right actions on the right resources.

Good access management applies the principle of least privilege without stifling those users and resources from legitimately accessing the resources they require to perform their jobs. Cloud IAM, as it's called in Google Cloud Platform, relies on strong identity management on the one hand (Cloud Identity) and clean and consistent resource management on the other hand (Resource Manager).

As such, access management deals with both natural users and service accounts, the bundling of both into user groups, and the assignment of the many IAM roles that group individual permissions together.

Architecture

Objective: providing best practice recommendations and a forward-looking view of the appropriate cloud compute and storage choices.

Cloud architecture ensures that applications take full advantage of the cloud platform capabilities and future-proofs the investment in a cloud migration by selecting appropriate compute and storage choices. For example, to achieve elastic scalability, cloud application architecture favors stateless (micro)services that are separated from persistent storage. Cloud infrastructure architecture employs software-defined, immutable components to assure repeatability and security by eliminating manual patching and maintenance.

It is an essential consideration for any business that wishes to achieve a step change in the scalability, availability, and affordability of their self-developed applications, data warehouses, and pipelines, and that seeks to increase development velocity as well.

Behaviors

Objective: developing a systematic way to understand and evolve the behaviors that teams and individuals need to demonstrate to improve willingness to work as a team, communicate with greater empathy for the audience, and retain more knowledge from upskilling programs.

Over 90% of our behavior is driven by our unconscious motivations, values, beliefs, and habits. For successful cloud adoption, it is critical to address not only the visible or conscious actions and rituals, but to also focus on the change required in mind-set and values. Your ability to learn and lead is predicated on the fact that people are going to adopt/demonstrate the new behaviours: e.g., collaboration, blamelessness, psychological safety, prototyping, data-driven decision-making.

The end goal is to enable organizations to understand current and desired behaviors and to develop a change journey that allows them to navigate this shift.

Continuous integration and delivery (CI/CD)

Objective: automating changes to the system through a CI/CD process pipeline, so that all changes can be tested, audited, and deployed with minimal interruption.

In a large, distributed system, there are a lot of unknowns, dependencies, and ownerships, which create uncertainty about whether code changes will work as intended. For businesses, uncertainty leads to risk and slows down software delivery. A continuous software release process that validates every change — continuous integration (CI) and continuous deployment/delivery (CD) — builds confidence that any code change will work as intended.

Cost control

Objective: instilling cost consciousness and soft boundaries with the consumers of cloud resources (architects, developers) by maximizing visibility into the costs incurred in near real time.

With no up-front procurement of IT resources to set a physical limit on the amount of resources that an application can consume and no capex-based, multiyear capacity planning, controlling costs begins with the individual software engineer. Physical limits of procured hardware are replaced by logical resource quotas and auto-scaling configurations. Without appropriate dashboards, alerts, and processes in place, managing the cloud expenditure for organizations with multiple projects, teams, or business units can be a cumbersome and time-consuming process.

In lieu of hard physical resource limits, application owners must choose from one of three strategies and take responsibility for enforcing it: unlimited scaling (e.g., customer-facing e-commerce), gradual service degradation (e.g., internal data analytics), or capped spending (e.g., developer sandbox).

Communication

Objective: understanding and managing a culture of blamelessness and open communication channels, where sharing failures openly is encouraged and mistakes are treated as opportunities for improvement.

In today's fast-paced and complex software delivery process, organizations need to understand that failure is inevitable and treat mistakes as opportunities for improvement. Creating a psychologically safe and blameless workplace, where taking interpersonal risks is encouraged and where the responsibility for mistakes does not fall on individuals, but instead on systems and processes, is essential.
Also key to this approach is the postmortem as a tool that helps promote a culture of blamelessness, continuous learning, and system improvement.

Data management

Objective: understanding and managing what data is being stored, where it originates from, how sensitive it is, and who is accessing it — for the purpose of keeping data safe, discoverable, and useful.

As an organization, being a good custodian of the data you hold is not just good practice. It makes good business sense as well. Poor data management can lead to breaches or other issues that can result in reputational damage for your business or regulatory sanctions. Encryption, classification, loss prevention, and adhering to regulatory compliance are just a few of the many considerations that fall under the umbrella of data management.

External experience

Objective: accelerating cloud adoption by applying best practices and other organizational lessons learned from day one, through experienced subject matter experts.

While knowledge can be gained through training and other means, the experience itself of building or implementing a solution provides insights and strategies to effectively overcome problems quickly, mitigate unforeseen risks, and develop best-fit solutions that address a specific business need.

In the early stages of a cloud adoption journey, seeking outside help is often a good strategy, whether from a Google partner, Google Professional Services, our Office of the CTO, or our solution architects.

Identity management

Objective: reliably authenticating users' or services' identity and guarding against loss of credentials and attempts at impersonation.

Establishing a person's or device's identity with absolute confidence is core to the modern security model in which no single factor is trusted -- not the password, not the certificate, and most certainly not the IP address — and yet, by combining many factors, can be trusted from anywhere on any network.

Incident management

Objective: alerting to, triaging, and rectifying unplanned service degradations in an orderly and timely manner, both self-sufficiently and with Google's support.

When operating a service, there is a strong requirement for efficient and effective delivery of support to business users and customers, and a requirement for quick restoration of service when things go wrong. In the case of adopting cloud technologies, there are both skill gaps and process gaps that need to be addressed to ensure optimized solutions, continued uptime, and business value.

The benefits of creating a rigorous support model include minimizing the risk of service outages, minimizing the impact of such outages when they do occur, and developing well-architected solutions that make the most of the tools and platforms on which they are built.

Infrastructure as code

Objective: automating through code the configuration and provisioning of resources, so that human error is eliminated, time is saved, and every step is fully documented.

Configuration and resource automation through code (also programmable infrastructure) enables horizontal and automatic scaling, locking down admin/root access to servers, provisioning developer environments within minutes, and switching over from one stable production version to another without downtime.

Instrumentation

Objective: measuring resource health and logging events, as well as tracing, profiling, and debugging applications, so that the behaviour of a system can be examined under any circumstance and service-level objectives can be quantified.

Comprehensive instrumentation, while essential in any IT operating model, plays an even more important role in the cloud. It provides the metrics by which an application will determine when and how to elastically scale its resources and provides crucial insights to help triage whether Google's services or your own application is the root cause for an observed poor performance or degraded service. Last but not least, and because every action in the cloud is an API call, comprehensive logging provides a gapless and immutable audit trail of who performed which action to which resource or configuration, which in turn helps make your cloud operations inherently more secure.

Networking

Objective: connecting and protecting services and the flow of data between them via logical boundaries, regardless of a service's identity or permissions.

Networking is a critical infrastructure component for any business. The network connects clients to servers or services, it connects a business to its customers, and it enables employees to complete their work. No business today can function without connectivity — not only within the organization's boundaries, but also to customers, partners, and the wider internet. This applies to businesses of all shapes and sizes, whether infrastructure is fully on-premises, all in the cloud, or a hybrid of both.

People operations

Objective: defining the required organization structures and aligning cloud adopters to the right role, skills, and performance measures to help them fulfill their new tasks and duties.

Alignment of the organizational structure, people, and performance measures ensures that teams are set up to receive the change and embrace their new duties. For example, a company could make a substantial investment in migrating to the cloud, but if the IT, operations, and related business resources don't know how to work with one another or know what is expected of them, then chaos can develop, negatively impacting the return on investment.

It is also important to ensure that cloud adopters are incented for executing their new responsibilities and behaviors (e.g., collaboration, transparency, acceptance of failure, trust) through the performance management process and incentive structures.

Finally, it is critical to set organizational goals that are both measurable and able to be influenced by the journey that the organization is on. Misaligned goals and initiatives will have a negative impact on the success of cloud adoption.

Resource management

Objective: organizing, naming, and setting quotas of cloud resources in order to ensure a structured, consistent, and controlled environment.

The ease with which resources can be virtually created in the cloud by almost anybody also poses challenges in maintaining a clear view and minimizing sprawl across the cloud account. Useful and simple naming conventions and a thoughtful folder and project hierarchy that mirrors the organization's hierarchy help to federate governance while avoiding anarchy.

Sponsorship

Objective: passionately and continuously demonstrating executive support for the cloud adoption strategy, so that early adopters have a widely recognized mandate for change.

Sponsorship refers to the active and visible support that executives and team leaders give to a cloud initiative or project within the organization. Enterprise cloud adoption is complex. Strong sponsorship is vital when organizations make the decision to go forward with organization-wide deployments of cloud platforms or applications whose intent is to add value and drive organizational collaboration and velocity.

As the most influential individuals within an organization, executives must passionately and continuously demonstrate executive support for the cloud adoption strategy, so that early adopters have a widely recognized mandate for change.

Teamwork

Objective: building a team that lives and breathes behaviors and culture, which includes high collaboration and trust, so that cloud technology is utilized in the most optimal manner.

Teamwork is driven by thought leadership from the bottom up, beginning with the individual contributor. This thought leadership can take many forms, such as a Center of Excellence, dedicated evangelist roles, or informal champions, and may involve many different avenues of knowledge sharing. Advocacy encompasses all IT disciplines, from security to architecture, from networking to operations and database administration. What they all share is a forward-thinking and self-motivated interest in cloud adoption best practices.

Without a critical mass of advocacy, all responsibility for generating cloud adoption momentum rests with the executive sponsors (see the Sponsorship epic). Such a one-sided, top-down push is not only slow to scale but also fails to capitalize on the inherent democratization of IT resources that cloud computing offers.

Upskilling

Objective: investing in learning, so that the incumbent staff may combine their existing in-depth knowledge about the business and the current IT estate with learnings about new best practices.

Cloud computing marks a paradigm shift in IT the likes of which the industry has not seen since the introduction of virtualization. These new principles and best practices can be studied in many different ways to suit your teams' individual learning styles, ranging from instructor-led training courses to self-serve interactive courses and quests with coursera.com and qwiklabs.com.

Upskilling is about more than just understanding the technical theory. It's about applying the learning on the job, self-sufficiently researching solutions to issues online, or reaching out to Google Support and sharing lessons learned with peers, so as to nurture a culture of continuous learning and to grow institutional knowledge.