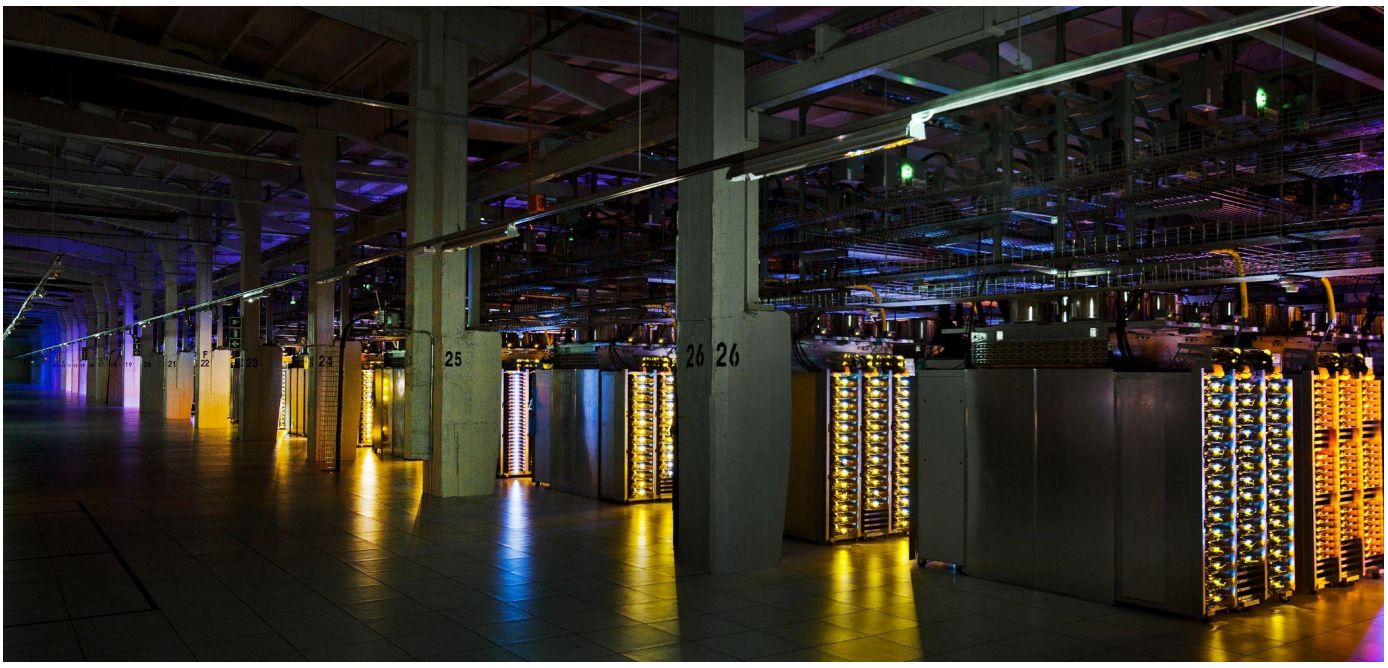
Google Cloud

CIS Center for Internet Security®

Office of the CISO

Securing and Scaling Cloud Adoption

A pragmatic approach to cloud adoption in U.S. state, local, tribal, and territorial (SLTT) government.



October 2024

Table of Contents

01

Introduction: How SLTTs envision leveraging cloud infrastructure

Mature state, local, tribal, and territorial (SLTT) organizations, with the appropriate IT talent to architect and select native cloud services, are interested in infrastructure as a service (IaaS). This type of cloud deployment may grow over time as the IT skill level of staff from less mature SLTT entities increases.

Software as a service (SaaS) deployment type is the most popular, likely because it does not require a lot of new cloud-specific skills to migrate existing SLTT software applications to run in a virtual cloud environment, especially if IT staff decide to migrate to, for example, Google Workspace productivity software. However, this is where SLTT entities get into overall cost and security challenges when using the SaaS deployment model. Securing the software application is the responsibility of the customer, not the cloud service provider (CSP), making this paper all the more relevant for those SLTT entities interested in securely migrating to the cloud.

In a poll surveying SLTT IT staff across the country, most shared a concern about the security of the cloud infrastructure itself and the security of their data in the cloud. The next highest concerns for SLTT entities considering migrating to the cloud were a lack of skilled resources and the cost to migrate.

While some SLTTs polled have already begun their cloud migration journeys, the vast majority (69%) indicated they do not have the internal talent to migrate to the cloud, highlighting the need to acquire consultants, augment their current staff, and recruit full-time employees to manage their cloud services.

Additional polling data also shows that SLTT government organizations indicate their top three key drivers for migrating to the cloud are disaster recovery, resiliency, and increased security/reduced risk.

And when it comes to services, email tops the chart, followed by additional services such as collaboration tools, unified communications tools, and file-sharing capabilities.

The state of the SLTT community

As with most industries, the advantages of moving SLTT organizations to the cloud are clear. You gain the opportunity to encourage and promote innovative new ideas. You also gain agility through an approach to information technology that carries less bureaucracy with it. Counter to prevailing concerns, cloud brings improved risk management and security to the overall fabric of your infrastructure. Cloud computing allows you to operate like a utility, much like your electrical, gas, water, and telephone services, with the same resulting efficiencies and cost effectiveness.

As you migrate to the cloud, what you gain in simplicity, security, and scalability builds confidence, trust, and reliability across your SLTT government organization.

The interconnection of cloud migration, digital transformation, and organizational transformation

Cloud migration is a key component of – and even a catalyst for – digital transformation. It brings with it the potential to liberate your organization from the challenges and costs associated with your legacy data centers. The velocity of change when it comes to cloud migration is fast, very fast. Think of the path of changes that took us from pay phones to mobile phones to smartphones. Cloud-driven change is proving to be even more accelerated.

It's a balancing act – your mission and new opportunities amid pressing challenges

Regardless of size or branch, every SLTT government faces similar imperatives. You want to improve public service and public safety services in your community, and you want to deliver these services in a timely, secure, and innovative way. At the same time, you aim to reduce cycle time and mundane activities increasingly with the use of process automation.

But the challenges around how you execute can be daunting.

Of course, like any public sector organization, yours is a traditionally people-and-paper oriented business that knows how to get the job done with current processes. But it's time for a change. Culturally, change is always hard, as your staff are comfortable with the status quo.

Talent shortages continue to abound, even for your legacy systems. And while the timing may seem right to move to the public cloud, it can be perceived as just another infrastructure that will stress your team. While you may need to increase or augment talent in the initial stages, you'll realize gains in the economies of scale and as you migrate workloads to the cloud.

From a technology perspective, your existing IT systems are often layer upon layer of equipment deployed over decades and incorporating everything from mainframes to Microsoft Windows servers. Consequently, comprehensive cybersecurity is much harder to establish when your current technology stacks are heterogeneous and complex. However, with cloud, cybersecurity is a primary component of installation from day one.

Where Google fits in your cloud migration journey

In this paper, we're taking a practical approach to cloud migration and security for SLTT government organizations.

As with other industry verticals, public sector customers can also leverage security best practices and the robust cloud infrastructure that Google has to offer. Our global technology infrastructure components – including disks, servers, networks, and information subsystems – are homogeneous, strictly controlled, and incorporate software-defined automation. It's the same secure global infrastructure that powers Google daily. This same infrastructure that powers Google's day-to-day services is available to your organization.

Transformation is about renovating, rethinking, reimagining, and revolutionizing how to provide better public services. Every organization is at a different phase of this transformation journey. If you're now running in the cloud on premises as an extension of your data center, managing that cloud can be more challenging and time-consuming than you planned for. Migrating to Google Cloud brings you the added business value that comes with our managed services. We can eliminate the burden of running IT infrastructure, without vendor lock-in, thanks to our open-source pedigree.

Importantly, Google Cloud is secure by design, with policy, controls, and enforcement engineering built into the fabric of Google Cloud. Google has been a security pioneer for decades and has driven the evolution of the security industry as a whole. We developed many of the current best practices, and we pioneered the enterprise application of zero trust principles. Today, Google keeps billions of people safe online with proactive security that's built in, not bolted on. We bring this same security expertise to Google Cloud for the public sector.

Partnering with Google, CIS is helping SLTT organizations with cloud migration journeys

As an independent and trusted nonprofit cybersecurity partner of public and private organizations around the world, the Center for Internet Security® (CIS) offers trusted, consensus-based best practices (CIS Critical Security Controls® and CIS Benchmarks™) that provide organizations of all sizes with specific and actionable recommendations to enhance cyber defenses.

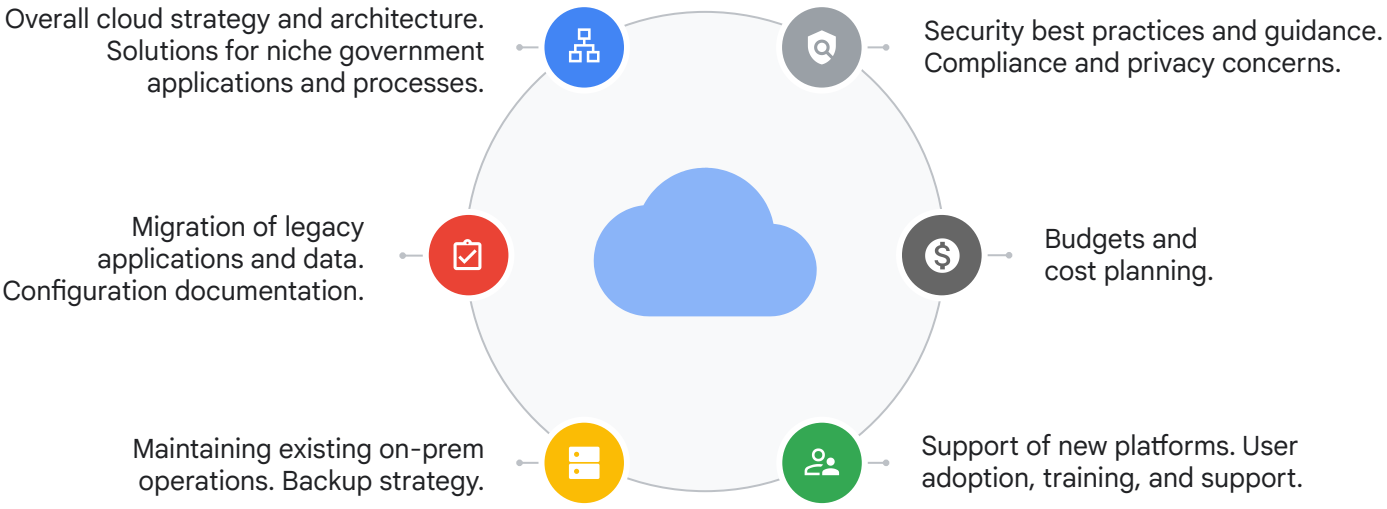
CIS, as the home of the Multi-State Information Sharing and Analysis Center® (MS-ISAC®) and Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), provides U.S. SLTT government organizations with no-cost and cost-effective cybersecurity resources and services to promote effective cybersecurity among the public sector.

CIS's dedication to helping the cyber underserved – many of whom are in the SLTT community – improve their cyber maturity is continually evidenced by the tireless efforts of its employees and global community of cybersecurity experts. These cybersecurity experts form the backbone of the globally recognized standard of best practices, including CIS Controls and CIS Benchmarks, for securing IT systems and data against the most pervasive attacks.

Whether CIS is surveying member needs on cloud adoption, vetting and adding new vendors to CIS CyberMarket®, or strengthening partnerships with established technology providers such as Google, their mission remains paramount: to make the connected world a better place.

By partnering with organizations such as Google and bringing the consensus-based security configuration recommendations of the CIS Benchmarks to the cloud via CIS Hardened Images®, CIS tees up SLTTs to begin, continue, or optimize their cloud migration journeys on Google Cloud Platform (GCP).

What challenges do you have for cloud adoption?



Creating a roadmap for your cloud adoption journey

Now we're going to take a closer, more prescriptive look at our recommendations for cloud migration and security for SLTT government organizations like yours. We'll start with a look at strategy and execution and address the critical nature of organizational and cultural change. Next we'll focus on technology platforms and the characteristics and advantages of Google Cloud security. We'll close with a broader look at establishing your own migration plan – one designed to safely operate at scale.

02

From strategy to execution – and everything in between

Here's the reality for today's IT departments in SLTT government: you are emerging from decades of overlapping government technology decisions. The result? You are now grappling with sedimentary hardware and software platforms that have created complex and fragmented environments in need of constant updating and maintenance to service your ongoing government operations. This in turn often requires human resources in thousands of discrete architecture, engineering, and operations disciplines all at a time when organizations are being asked to do more with less.

What's more, you're facing the constantly increasing need to deliver timely, innovative services to your community and improve public service and safety services, coupled with additional needs to reduce mundane activities and cycle times through process automation. At the same time, you're facing demands for greater speed when it comes to transforming new technology-based ideas to functioning systems, measured in weeks, not years.

To further complicate matters, people, places, and things related to your organization can be located anywhere, both physically and virtually. This puts more pressure on your IT team to deliver services with strong data security, privacy, compliance, risk management, and comprehensive monitoring. Accomplishing all this is not always simple and fast. Moving to the cloud is often part of the solution.

Tackling the unique cloud challenges for SLTT governments

When SLTT organizations talk about moving to the cloud, a familiar response is, "Move to the cloud? Now? How are we going to do that?" Built on deep experience, Google understands the challenges that come with transformation in the public sector.

Think people, process, then technology

Urs Hölzle, senior vice president of technical infrastructure here at Google, has said, "The story of transformation is a human one that involves as much cultural transformation as technological transformation."

Never underestimate the challenges of successfully running cloud migrations. While such a transformation is well worth doing (and perhaps even necessary for regulatory or policy reasons), the effort behind it can be strenuous. Success demands everything your organization can give collectively.

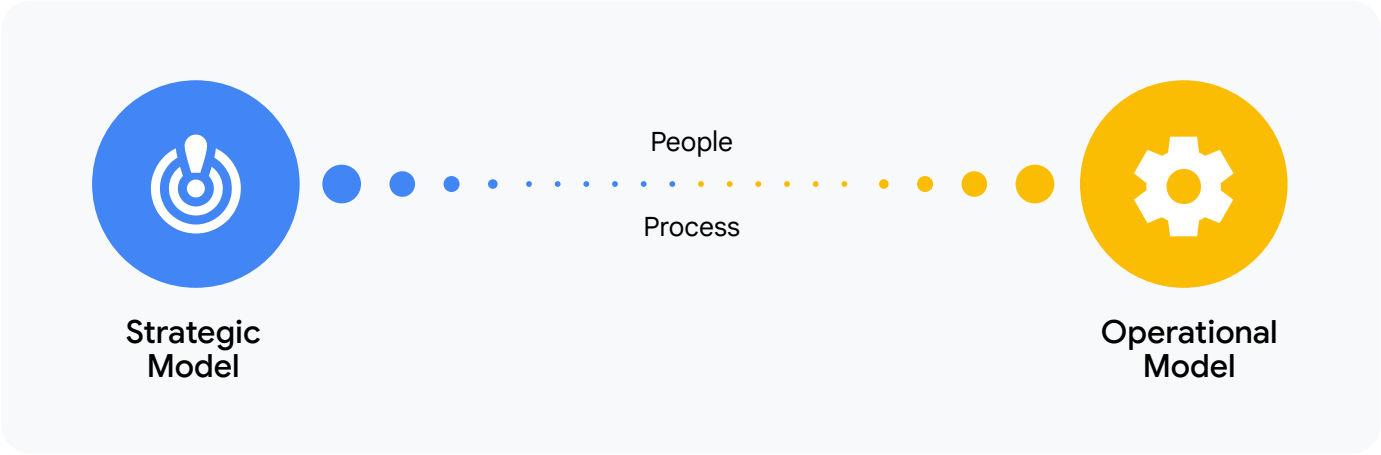
You can start with, not a strategy per se, but more of a way to approach your strategy. For this to work, what you prepare to share within your organization should be simple, direct, and clearly indicate how your approach to the strategy effectively solves the challenges of migrating to the cloud. If the basic strategy and how that strategy benefits the organization cannot be communicated to a roomful of stakeholders in under ten minutes, you need to revisit and rework it.

Being able to share the overarching strategy with your non-technical teams can be helpful. Cloud services will have a significant impact on, not only the citizens in your community, but also your administrative teams, including human relations, policy management, auditing, and security.

Taking the first steps from strategy to operational model

Cloud migrations are not an all-or-nothing process, and there's no requirement that your entire organization must migrate to the cloud to enjoy significant benefits. While a clear and direct plan is recommended, the first step could be as simple as an exploratory step to move one low-risk, low-value, and read-only application into the cloud, performing a post mortem, and then making a more comprehensive plan based on the lessons learned.

It may very well be the case that select services can be moved without undue disruption or excessive effort. By limiting the scope of proposed change to well-understood domains, such as citizen-facing applications and portals, individual thought leaders within your organization can have a visible impact on modernizing your working environment – all while showing a technical path forward to leadership teams. This approach also provides the architecture and engineering specialists with an opportunity to learn and upskill before further cloud migrations as you move from your strategic to operational model.



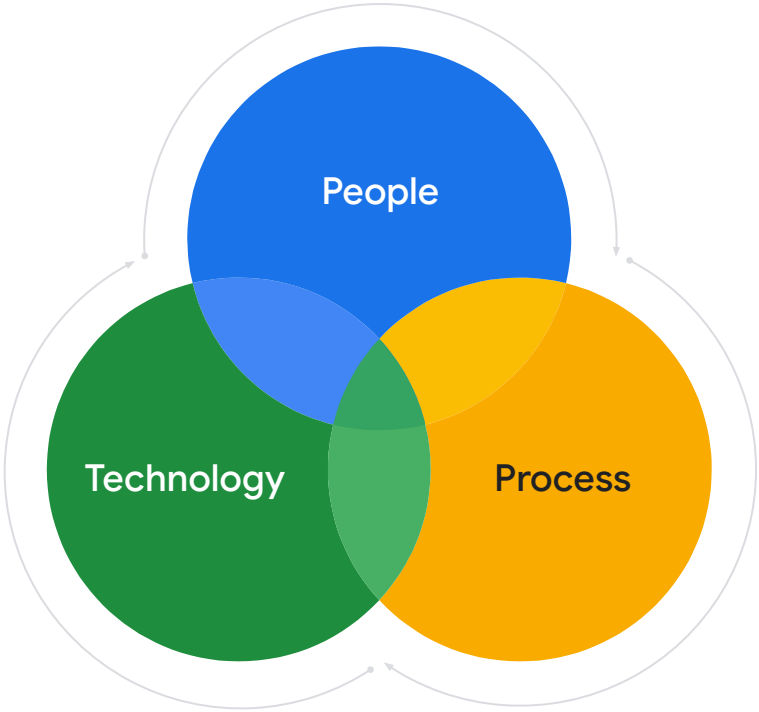
Be realistic as you move ahead

Consider this popular adage: "Slow is smooth; smooth is fast." It's a way of emphasizing that it's important to be realistic in the initial planning stages. A very high percentage of major IT initiatives either fail outright or are in limbo. In fact, Gartner predicts 80% of data and analytics governance initiatives will fail by 2027 due to a lack of a real crisis (like COVID 19) or a manufactured one. In many cases, projects are rescued before they fail so some form of "victory" can be declared.

The most common migration failures occur when you're trying to do too much too soon on a tight schedule. When little is understood about the new platform, the organization is more likely to experience failure and then give up. Alternatively, when you start small with strategic, low-hanging fruit, you're much more likely to achieve modest early victories, learn from them, and then move on with your transformation. It's a tried-and-true principle, and it certainly is applicable to cloud migration: learn from the experience, and only then begin broader planning.

What's not to like? How to think about cloud migration.

As we've discussed, executing your cloud migration is more than simply introducing new technology. It requires the interplay of people, process, and technology.



As a word of caution, focusing on the coolest cloud technology with a proprietary vendor product suite should be considered less than ideal. In reality, it can be very restricting. Technology can be like the fashion industry with trends moving in and out of vogue, methodologies rising and falling, and the leading edge of today becoming the technical debt of tomorrow.

Challenges

Today's IT environment

A multigenerational complex collection of parts assembled over several decades that is increasingly difficult to run and operate and possesses a rigidity and challenge to extend to meet new government product and service demands.

Solution

Migrate cloud computing

A promising IT paradigm that can lead to lower fixed costs, a more flexible allocation of resources, faster development, broader reach, a safer change control process, and faster time-to-value for public and government products and services.

Lean in to the inherent benefits of cloud computing

IT in government organizations is a critical enabler that supports your core interests – from public service innovation to robotic process automation. Cloud migration does not change that responsibility. Cloud computing, at its core, remains true to data processing. And by that fact, cloud computing is not revolutionary but evolutionary.

A core expectation, coupled with the primary value proposition, is that your cloud environment should not compound today's challenges by making service delivery even more complex, complicated, or expensive. Your cloud should instead provide a reliable, hardened platform that instills confidence at every touchpoint while being simple to use, secure by design, and scalable to meet known and unknown technology demands.

Let's continue to discuss what steps are needed to help you accomplish this – and how Google can help.

03

Fostering and evolving (necessary) organizational and cultural change

> “It’s good enough for government work.”

This expression is thought to have originated during World War II to highlight work that far exceeded rigorous standards. Over the years, the meaning has changed. Today, it’s often associated with an adequate or imperfect situation that is deemed not worth the effort to improve. And that phrase can certainly sting. To counter that perception, change is needed.

But change is hard – and that certainly includes the changes that come with cloud migration. Some are tempted to avoid this kind of change, not wanting to disrupt tried-and-true processes and the people who use and support them. So why rock the boat? Because, while change can be challenging, everyone applauds progress and the resulting improvements to public services.

In transitioning to the cloud, you’re asking stakeholders and staff to learn new technologies and apply them. For example, a user might need to learn a new tool or workflow, or a technologist might work with a new language or infrastructure.

Your end goal is to create a positive impact with cloud migration. That’s all about strategy and vision, but it’s also dependent on delivering a holistically better situation for your teams. Encourage a group effort with collective agreements to rise above the status quo in support of new processes and technology.

How you approach change can drive success

Whether of benefit to the public you serve, an agency, or internal operations, the more people who benefit from change, the more likely it will succeed.

In fostering organizational and cultural change, consider developing the following three dimensions:

01

Identify what’s good for your organization.

02

Define the execution pattern.

03

Rethink how engineering and operations teams partner.

Let’s delve into these three areas a bit more.

01

Identify what's good for your organization

What is "good" in this context? Defining it in terms of your organization involves making a new process or program that is easy to understand, measure, and communicate. It sets the bar and provides a practical description of all aspects that are needed to make the vision a reality.

Defining "good" for your organization will typically rally around two dimensions:

- **A business context** to explain the desired outcome and cast a vision. This helps drive momentum.
- **A technology context** of why technology is in its current state and the net positive value of the future state.

Whichever approach you take, it's important to establish it from the very start of your cloud migration project. As the Peter Principle posits, "If you don't know where you are going, you will probably wind up somewhere else."

02

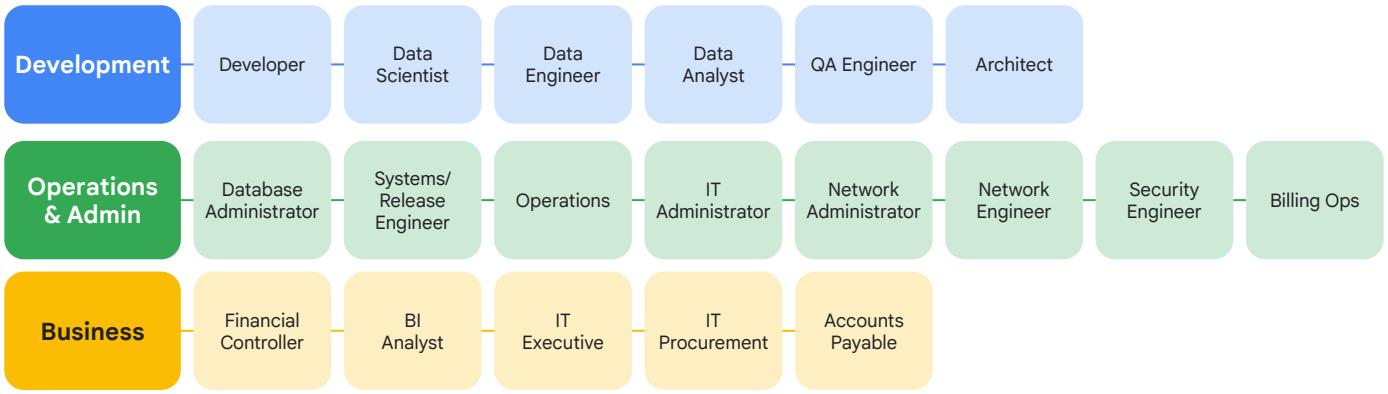
Define the execution pattern

First take the time to understand the roles across the cloud migration program. Roles are diverse and often structurally and organizationally spread across three categories: development, operations & admin, and business.

Development
Develop applications and services in support of internal and external customer and business needs

Operations & Admin
Define, create, and manage the overall IT infrastructure in support of application and service development

Business
Use cloud products in support of business needs and objectives and guide adoption



Application development teams should be accountable for the entire value stream from design to production. However, owning the entire value stream requires a wide array of disciplines and mastery of technologies involving multiple roles such as developer, data scientist, and data analyst.[1]

You want to develop teams based on these key characteristics:

- Approach software engineering as a team endeavor. It's not about individual heroics but about working as a unit. Use balanced teams to deliver products.
- Foster collaboration among project managers, engineers, and UX designers.
- Mitigate the risk of errors by fostering a working environment that promotes authentic human connection.
- Shrink the number of distinct roles.
- Capture metrics that matter with a focus on product health and usefulness, with engineers also tracking aspects like quality.

When it comes to cloud migration and maintaining "what is good" across all roles and responsibilities in your organization, consider this straightforward three-part pattern:

01 **Set end goals based on business value.** This becomes your North Star vision against which all other decisions are made. It's foundational and casts a vision for what the organization wants to become.

02 **Every aspect of your North Star vision gets an action plan** devised of sprints, which outlines where things are today and the required objectives and resulting milestones needed along the way to get to the desired end state. Even if you don't yet know how you'll accomplish each milestone, it's essential to lay out the road map. At a minimum, milestones often cover people, process, and technology for completeness.

03 **Each milestone is defined by a set of objectives and key results** (OKRs) that are assigned to the responsible group or groups. Depending on the complexity, key results are often best expressed as a key performance indicator (KPI), which allows you to measure progress toward the North Star vision. In many cases, if it isn't a number, you can't measure it, and you won't know if you're making progress.

Establishing a value-based vision translates to the creation of what's needed to fulfill the vision. You can then build a road map composed of incremental milestones, with each milestone defined by OKRs to make it concrete and real.

[1] Lean Enterprise (O'Reilly) by Jez Humble, Joanne Molesky, and Barry O'Reilly, 2014.

03

Rethink how engineering and operations teams partner

Site reliability engineering (SRE) is a set of principles and practices that applies aspects of software engineering to IT infrastructure and operations. Simply put, SRE is what you get when you treat operations as if it's a software problem.

At Google, we look at SRE as a way to rethink how your engineering and operations teams can partner during and beyond cloud migration. Our mission is to protect, provide for, and progress the software and systems behind all of Google's public services – Google Search, Ads, Gmail, Android, YouTube, and App Engine, to name just a few – with an ever-watchful eye on their availability, latency, performance, and capacity.

With SRE, you can reap the benefits of speed as you improve reliability with proven SRE principles.

Now let's examine what's needed for your cloud technology platform.

04

Establishing a hardened, resilient technology platform

Start with building on key characteristics that ensure a technology platform that delivers security, reliability, recoverability, adaptability, and effective monitoring.

Security is paramount. Incorporating robust measures to protect against unauthorized access, data breaches, and cyberattacks must be part of all your cloud security plans.This includes strong encryption, multi-factor authentication, intrusion detection systems, and regular security assessments.

Reliability, recoverability, and adaptability are equally important. Reliability ensures consistent performance and availability of the platform, minimizing downtime and disruptions. Redundancy, fault tolerance, and load balancing are employed to maintain high levels of service. Recoverability is all about your ability to quickly restore operations after a failure or disaster. This involves having comprehensive backup and disaster recovery plans in place, and regularly testing these procedures. Adaptability allows your platform to evolve with changing business needs and technological advancements. Modular design, scalable architecture, and the ability to integrate new technologies are essential for long-term viability.

Cross-platform monitoring provides real-time visibility into the platform's health and performance. This enables proactive identification of issues, optimization of resources, and early detection of security threats. By employing robust monitoring tools and practices, organizations can ensure the continuous and efficient operation of their technology platforms. Incorporating these capabilities enables multiple benefits:

01

Enhanced security with a hardened platform fortified against cyberthreats, reducing the risk of data breaches, ransomware attacks, and other security incidents. This safeguards sensitive information and ensures business continuity.

02

Improved reliability minimizes downtime and disruptions, ensuring consistent performance and availability of critical systems. This leads to reduced service disruptions, which in turn increases public trust, enhances service delivery, and allows for better resource allocation.

03

Rapid recovery in the event of a disaster or system failure enables swift recovery of data and operations. This reduces downtime, minimizes financial losses, and maintains business continuity.

04

Adaptability to change means you can more readily adapt to evolving business needs and technological advancements. This ensures that the platform remains relevant and effective in the long run, reducing the need for costly replacements or upgrades.

05

Long-term cost savings come from reduced downtime, improved security, and increased operational efficiency, all contributing to a lower total cost of ownership.

Your cloud technology platform is set. But is it truly secure by design?

05

Secure by design for seamless, pervasive, and omnipresent protection

Security is not an afterthought but a fundamental consideration at every stage of development and deployment. As defined in the paper titled Secure by Design: Shifting the Balance of Cybersecurity Risk, "secure by design" means that technology products are built in a way that reasonably protects against malicious cyberactors successfully gaining access to devices, data, and connected infrastructure.

What comprises security by design? Consider:

Threat modeling – Identifying potential threats and vulnerabilities early in the design process allows for proactive mitigation and reduces the risk of security breaches.

Secure coding practices – Implementing established coding standards and best practices minimizes the introduction of vulnerabilities and bugs that could be exploited by attackers.

Security testing – Testing throughout the development life cycle helps identify and address security flaws before the platform is deployed, ensuring a more robust and resilient system.

Default security – Setting secure default configurations and options protects users out of the box, reducing the risk of misconfiguration or human error leading to vulnerabilities.

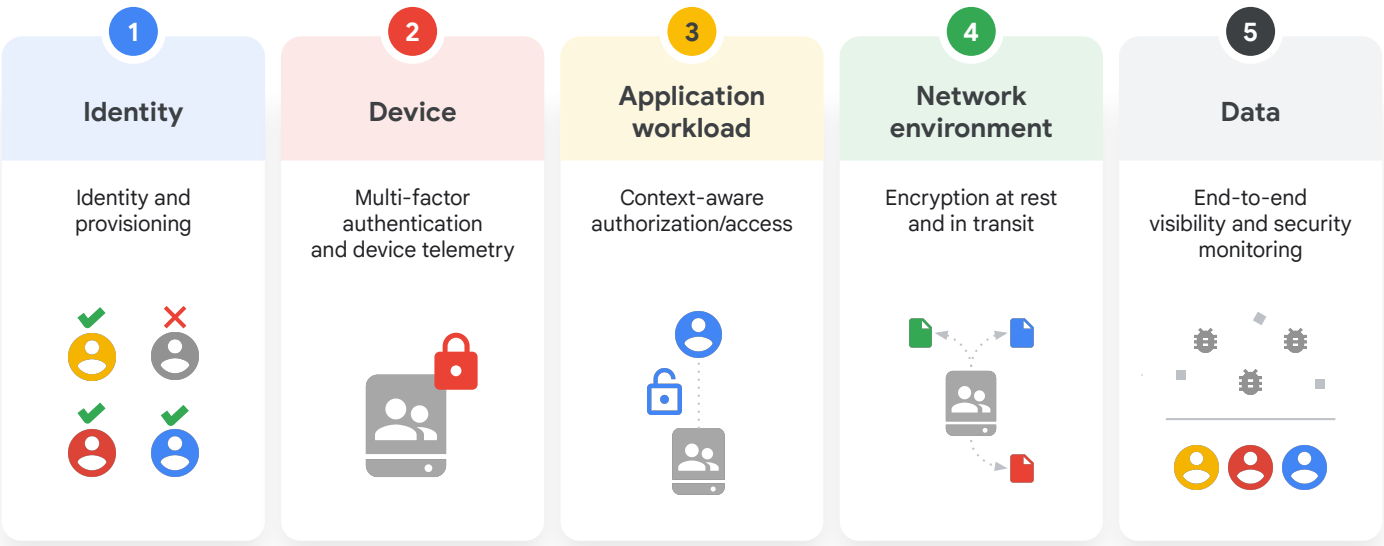
Layered security – Making sure security is not an afterthought but rather integrated into every layer of the system, from hardware and firmware to software and cloud infrastructure.

Data protection – Implementing measures to protect data at rest, in transit, and in use through encryption, access controls, and data loss prevention techniques ensures data confidentiality, integrity, and availability.

By adhering to these principles, your organization can create technology platforms that are inherently secure and resilient, minimizing the risk of security incidents while protecting valuable assets.

Zero trust plays an important role here. This is the security model used to secure an organization based on the idea that no person or device should be trusted by default, even if they are already inside an organization's network. A zero-trust approach aims to remove implicit trust by enforcing strict identity authentication and authorization throughout the network, not just at a trusted perimeter. Every request to access resources is treated as if it comes from an untrusted network until it has been inspected, authenticated, and verified. Trust needs to be established via multiple mechanisms and must be continuously verified. Embarking on a zero-trust architecture journey gives you in-depth defense, with the ability to methodically shut down attack vectors.

Google pioneered zero trust by globally implementing perimeter-less security for itself based on context-aware least privilege. Government agencies rely on Google zero-trust capabilities for remote access, secure collaboration, and boundary security. For example, Google offers professional services to help you accelerate government compliance, along with partnerships to help meet EO 14028, OMB M-22-09, and NSM-8. The zero-trust model presented below maps to the various security components as per NIST Zero Trust Architecture and CISA Maturity Model.



Now, how do you put your cloud migration strategy into action?

06

The challenges of transformation: Guiding your migration program

As John P. Kotter states in his book Leading Change, “Transformation is a process, not an event.” And it’s not without challenges.

A comprehensive technology migration program must strategically address hardware, software, and cloud resources to ensure optimal performance and minimize disruptions.

When it comes to hardware in your data center, a well-defined lifecycle management process is crucial. This involves continuous monitoring of hardware performance and health, proactive replacement of aging components before failure, and planning for capacity upgrades based on anticipated needs.

Regular software upgrades are essential to maintain security, compatibility, and access to new features. Rigorous testing in a controlled environment before deployment is vital to prevent unforeseen issues. For legacy software, evaluating replacements may be necessary to avoid compatibility and support problems.

Continuous monitoring of cloud usage and costs helps identify inefficiencies and optimization opportunities. For flexibility, a hybrid model that allows seamless migration between on-premise and cloud environments based on demand, cost, or performance considerations can be implemented.

By addressing these aspects, your technology migration program can facilitate a smooth transition, minimize downtime, and ensure that the organization's technology infrastructure remains modern, efficient, and aligned with evolving business needs.

Recommended steps to take

A successful technology migration program hinges on a well-structured, multi-step process:

01 **Analysis** – Thoroughly assess the current technological landscape, identifying pain points, redundancies, and opportunities for improvement. This phase sets the foundation for a targeted migration strategy.

02 **Planning** – Develop a detailed roadmap outlining timelines, resource allocation, potential risks, and mitigation strategies. A phased approach may be adopted for complex migrations.

03 **Testing** – Rigorous testing in a controlled environment is crucial to identify and resolve any compatibility issues, performance bottlenecks, or unexpected behaviors before the new technology goes live.

04 **Deployment** – Execute the migration plan, ensuring minimal disruption to ongoing operations. This phase may involve gradual rollouts or phased implementations, depending on the scale and complexity of the migration.

05 **Training** – Create comprehensive training programs to equip users with the necessary skills to navigate the new technology effectively, fostering smooth adoption and maximizing productivity.

06 **Monitoring** – Continuously monitor post migration to ensure optimal performance, identify lingering issues, and enable proactive adjustments as needed.

07 **Reviewing lessons learned** – Apply lessons learned at every step as you fine-tune processes and promote a perpetual change attitude.

By following these key steps, your public sector organization can ensure a seamless technology migration program that minimizes risk, maximizes benefits, and drives long-term success.

Successful transformation hinges on adopting a perpetual change attitude

Moving forward with a mindset that is cultivated to foster continuous improvement and adaptation of new technologies and processes is to everyone's advantage. Your organization can best achieve this through agile methodologies that embrace agile principles, enabling your teams to iterate quickly, adapt to change, and deliver value incrementally. This promotes a culture of flexibility and responsiveness to evolving needs.

Openness and proactiveness are key. Fostering an environment intentionally designed to encourage people to connect with each other, engage in open communication, and collaborate across teams and departments is the key to seamless implementation. Employees who feel stronger connections with their colleagues make fewer mistakes, are more productive, and actively break down silos to facilitate knowledge-sharing and innovation. An open mindset is key to embracing new ideas and approaches. Rather than reacting to problems, encourage the value of taking a proactive stance by anticipating potential challenges and opportunities. Celebrate those who identify challenges and opportunities for improvement. Regularly assess your technology landscape and explore emerging trends to stay ahead of the curve.

You also need to continuously evaluate your processes, tools, and technologies to identify areas for optimization. Regular feedback loops and retrospectives can help you learn from past experiences and refine your approach.

At the end of the day, your security measures should be integrated in a way that doesn't disrupt the user experience or workflows. You can reduce the burden on your users and administrators by automating security tasks like updates, patches, and vulnerability scans. Use continuous monitoring of systems and networks to detect and respond to security threats in real time. And always apply secure, user-friendly authentication processes like biometrics and single sign-on, and authorization based on roles and permissions.

07

Safely operating at scale

Operating safely at scale across your organization (no matter its size) requires a multi-faceted approach that combines technology, processes, and people.

Primarily, a secure and robust infrastructure is the foundation. This includes hardened systems, regular patching, and proactive vulnerability management. Complementing this, an effective threat monitoring program provides real-time visibility into potential threats, allowing for swift incident response.

But technology alone is not enough. Organizational security awareness is crucial. Employees must be trained to identify and report suspicious activity and understand their role in safeguarding sensitive data.

To adapt to modern demands, cloud-native architecture offers scalability and flexibility while planned resilience ensures business continuity in the face of disruptions. Adopting a zero-trust access model further minimizes risk by verifying every user and device before granting access.

Security is paramount. Leveraging artificial intelligence (AI) and machine learning (ML) enhances the efficiency and effectiveness of the security components of your cloud migration. These technologies can analyze vast amounts of data to identify patterns and anomalies that might indicate potential threats, helping security teams stay one step ahead. As an example, Google Threat Intelligence combines the unmatched depth of our Mandiant frontline expertise, the global reach of the VirusTotal community, and the breadth of visibility only Google can deliver, based on billions of signals across devices and emails. Combining this comprehensive view of the threat landscape with Gemini AI supercharges the threat research processes, augments defense capabilities, and reduces the time it takes to identify and protect against novel threats. (Note: Some components of Google Threat Intelligence are incorporated into different security solutions. It is also available as a standalone paid offering to customers.)

08

Avoiding common pitfalls

A successful cloud migration requires careful planning and consideration of common pitfalls that center around:

01 **Lack of adequate planning** – A well-defined migration strategy with clear objectives, timelines, and resource allocation is crucial. Neglecting this step can lead to delays, cost overruns, and unforeseen complications.

02 **Network infrastructure and security** – Assess your network's readiness for cloud integration, ensuring adequate bandwidth and security measures to protect data in transit and at rest.

03 **Cloud security risks** – Cloud environments introduce unique security challenges. Familiarize yourself with these risks and implement appropriate security controls to safeguard your data and applications.

04 **Data migration challenges and loss** – Plan for efficient and secure data transfer, considering data integrity, encryption, and potential downtime during migration.

05 **Cloud compliance requirements** – Understand and adhere to relevant industry regulations and compliance standards to avoid legal and financial repercussions.

06 **Budget control** – Establish a realistic budget that accounts for migration costs, ongoing operational expenses, and potential hidden fees. Monitor and adjust spending regularly to avoid surprises.

07 **Cloud selection and technology lock-ins** – Consider choosing a cloud provider and services that align with your specific needs, and avoid vendor lock-in by selecting solutions that offer flexibility and portability.

By addressing these potential pitfalls proactively, you can ensure a smooth and successful cloud migration that delivers the desired benefits while minimizing risks.

09

Conclusion: Migrating to the cloud with confidence

Your state or local government organization can successfully migrate to the cloud by embracing digital transformation with openness and a willingness to learn and adapt. Recognizing the potential of cloud technology to transform service delivery, streamline operations, and improve citizen engagement is key.

It's essential to develop a comprehensive migration plan that outlines clear objectives, timelines, and resource allocation, prioritizing workloads based on criticality, data sensitivity, and dependencies. Investing in training and development to equip staff with the skills needed to manage and operate in a cloud environment is also crucial. This includes technical knowledge, security awareness, and change management skills.

Starting with a pilot project to test the waters and identify potential challenges allows for refining strategies and approaches for larger-scale migrations. Be sure to leverage the expertise of cloud providers, consultants, and peers in SLTT government organizations who have successfully migrated, research available resources and best practices, and empower yourself with the knowledge needed to support informed decision-making.

By embracing an open attitude and taking a strategic approach, you can overcome barriers, minimize risks, and unlock the full potential of cloud technology to modernize your IT infrastructure and better serve your constituents.

Google Cloud is here to help you achieve a simple, secure, and scalable cloud migration for your SLTT organization.

Helpful resources

Gather online information on Google Cloud for U.S. government cybersecurity.

Check out this blog Introducing Google Public Sector.

Listen to the weekly Google Cloud Security podcasts to hear industry experts discuss some of the most interesting aspects of cloud security.

Read the paper on how AI can reverse the defender's dilemma.

About Google Cloud Office of the CISO

The Google Cloud Office of the CISO (OCISO) is the world's premier security advisory team, supporting the security and digital transformation of enterprises, critical infrastructure, and governments. We provide program management and professional services support, including transformation workshops and educational content. We map our global compliance certifications to industry control frameworks, enabling you to simplify your compliance journey, and can advise on specific mappings as part of onboarding or growth of your workloads. And we design and curate resources for CISOs and boards of directors on cybersecurity, risk governance, and secure transformation to support our customers and their leadership teams.

About CIS

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Critical Security Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyberthreat prevention, protection, response, and recovery for U.S. state, local, tribal, and territorial (SLTT) government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. election offices. To learn more, visit CIS or follow us on X: @CISecurity.

About MS-ISAC

The Multi-State Information Sharing and Analysis Center® (MS-ISAC) has been designated by the Cybersecurity and Infrastructure Security Agency (CISA) as the key resource for cyberthreat prevention, protection, response, and recovery for all U.S. state, local, tribal, and territorial (SLTT) governments. The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's SLTT governments through coordination, collaboration, cooperation, and increased communication. The MS-ISAC is a division of the Center for Internet Security® (CIS®), a 501(c)(3) nonprofit. Visit https://www.cisecurity.org/ms-isac/ or email info@msisac.org for more information.

About EI-ISAC

The Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®) works in support of the Cybersecurity & Infrastructure Security Agency (CISA) to provide election offices an election-focused cyberdefense suite, including sector-specific threat intelligence products, incident response, threat and vulnerability monitoring, cybersecurity awareness, and tools for implementing security best practices. The mission of the EI-ISAC is to improve the overall cybersecurity posture of all U.S. state, local, tribal, and territorial (SLTT) election offices through collaboration and information sharing. The EI-ISAC is a division of the Center for Internet Security® (CIS®), a 501(c)(3) nonprofit.

Visit Election Security Tools & Resources or email elections@cisecurity.org for more information.

Contributors

Written collaboratively, our paper on securing and scaling cloud adoption for SLTT government organizations comes from experience working with many customers in the public sector and the deep insights they've shared with us.

Bhanchand Prasad
CISSP, CAP, PMP, Google Certified Security Professional
Google Cloud Public Sector

Aaron Perkins
M.S., CISSP, Director of Communications
Center for Internet Security

Dr. Autum Pylant
Communications Manager
Technical Review
Center for Internet Security

Don Freeley
Vice President, IT Services
Technical Review
Center for Internet Security