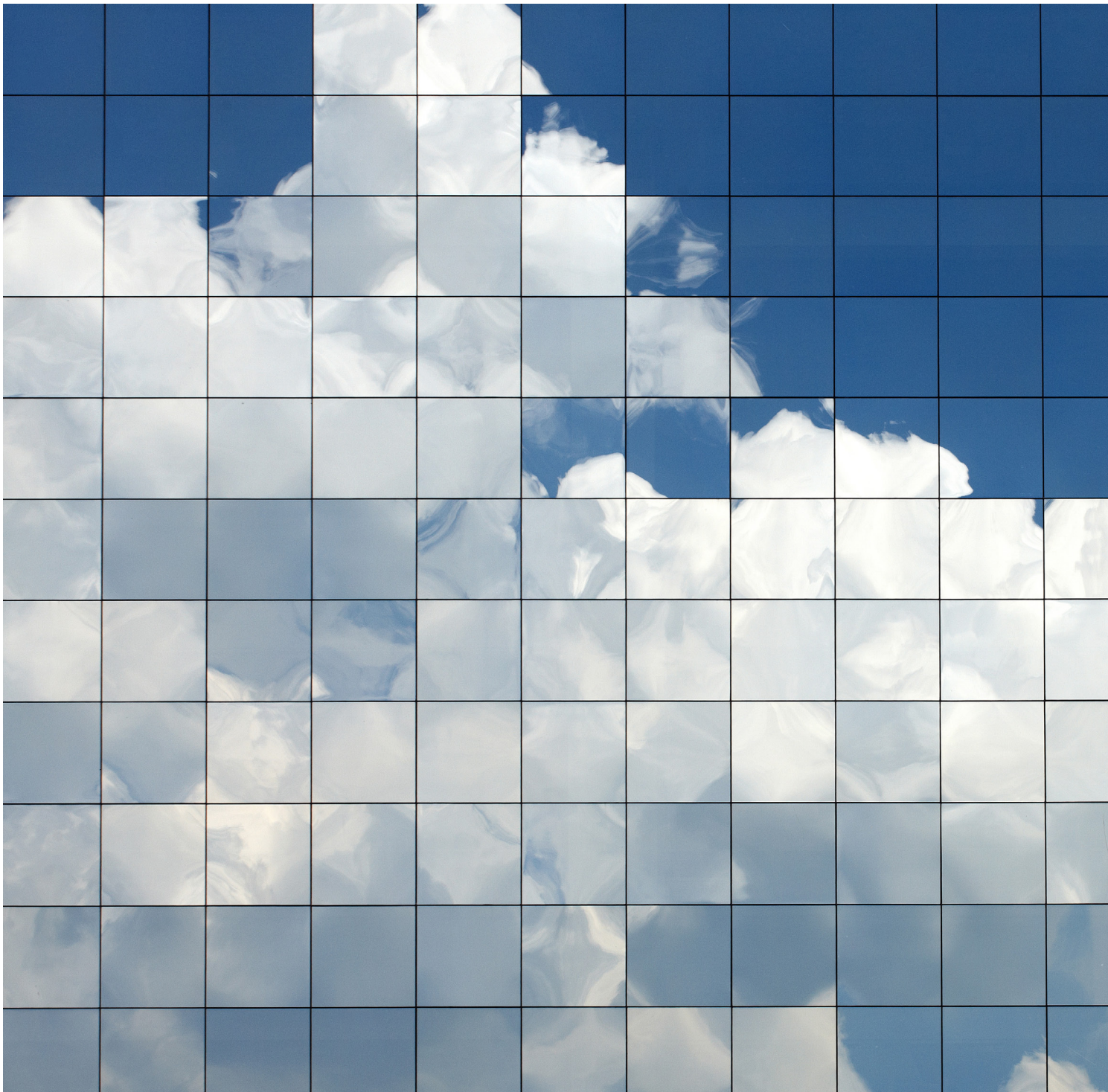
WHITE PAPER

CompTIA
Public Sector Procurement Council

Buying Cloud Guide



A Modernized Framework for Buying Cloud

First, it is not about "buying" cloud. Cloud is a critical enabler, and important for your digital transformation. The importance of cloud is not cloud itself – it is cloud's place in helping you accelerate, improve and exceed your organizational vision and objectives while securing your data.

Though costs can be reduced in many workload scenarios, a large cost benefit is the change in the way IT resources and services are consumed in the Cloud that can allow new funding strategies, creating budget efficiencies over the life span of the workload. Your digital strategy is what is most important. A strategy that drives towards agile, secure, data-driven decision capabilities allowing all members of your organization to deliver unparalleled services and outcomes for our citizens, partners and nation.

Cloud has become a vital component of successful digital transformations. Cloud empowers organizations to build, run, optimize, shift, scale and secure capabilities at speed and viewable costs with requisite resilience. Cloud helps navigate a time of exceptional challenge and change. As demonstrated in recent years, enterprises realized massive benefits and scale through the utilization of cloud platforms, which has facilitated and massively accelerated the shift to the remote workforce, supported new customer demands and sustained operations under severe disruption.

In 2013, CompTIA published ***"TechAmerica Foundation Cloud Buyer's Guide for Government"***. It is important to note though the fundamental principles of cloud value remain relatively the same, there is an important shift from the legacy "Cloud-First" strategy to the now relevant "Cloud-Smart" strategy. It is not just about having "cloud," rather how to fully actualize the promise and potential of cloud-native offerings while ensuring thoughtful execution that incorporates practical realities. To fully embrace cloud computing, public sector agencies should carefully evaluate the cloud services and solutions in the market to determine which ones meet their needs and move to implement them where appropriate. Recent developments in hybrid cloud observability solutions work across on-premises and multi-cloud environments and will optimize performance and reduce remediation by increasing visibility and productivity.

Buying cloud services is unlike most traditional technology purchases in government. Individual agencies have different requirements and demands of their cloud solutions, and as such it can sometimes be difficult to correctly procure cloud services. As federal, state, and local governments shift towards this new way of obtaining computer services, they need to design their strategies and solicitations so they harness the full power of the cloud business model. This Buyer's Guide white paper is designed to assist government agencies in navigating the process of acquiring cloud solutions as part of the digital strategy and transformation efforts.

Key Tenets of a Cloud Purchase

- **Start with the Business/Mission Results in Mind -** Begin with a business vision that outlines business/mission, performance objectives and overall goals; not with a particular cloud model (public, private, hybrid or community) pre-determined. It is important to not be proscriptive in drafting cloud requirements. Focus on business outcomes, expected service level minimums, and remain flexible enough to allow vendors to craft a variety of cloud solutions to meet requirements. Service level agreements that address not only availability, but performance can better plan meeting mission requirements.

- **Interoperability and a Unified Data Model –** Enterprises can benefit from multi-cloud architectures, with different areas of the business having the ability and flexibility to deploy on different cloud platforms as needs arise. Using multiple clouds can bring compelling benefits, with enhanced workload performance, reduced service disruption and vendor diversification ranking high among them. In planning your cloud purchases, pay special attention to interoperability, data ingress/egress requirements, visualization requirements, and your desire for automated intelligence and remediation. When cloud resources from multiple providers are connected, orchestrated and secured in a harmonized way, workloads run in unison to drive business agility, resolve problems, reduce costs and harmonize processes, making the multi-cloud a valuable place to be. If not planned properly, they can cause cost and complexity to soar. For multi-cloud initiatives to succeed, interoperability and a unified data model are key.

- **Understand the Security and Privacy Requirements –** Security and privacy are top concerns in today's complex and ever-changing IT environments. These two critical elements depend on technology, policies and practices. In your purchase of cloud services, pay special attention to the available security and privacy controls to ensure that the inherited, shared and user managed controls allow you to implement in line with your requirements. You should ask about a vendor's secure development lifecycle approach, what internal processes it uses to validate product changes, what internal processes it follows to identify insider threats and what the procedures are if a vulnerability is discovered. One must get a thorough understanding of the software build process, infrastructure, identity and access management, data protection, government/provider information sharing agreements and adverse event processes and knowledge sharing. Ensure a thorough understanding of your data rights provided by prospective cloud vendors Lastly, a robust security plan of your cloud services is essential in meeting business/mission outcomes. Ideally, you can find a vendor which offers solutions where security is built in the design from the beginning rather than bolted-on later through a patch.

- **Cloud Native and Composability Aspects –** Leveraging cloud services that have adopted components with which your team is familiar will accelerate migration, portability and implementation for cloud workloads. In addition, development organizations should look for cloud providers that offer cloud-native products. This will reduce time spent on operational tasks such as managing Kubernetes clusters, build applications faster and ensure deployed applications are more portable and can run on cloud products, on-premises environments or hybrid environments with minimal modification. Special attention should also be given to any open-source tools or applications currently used that are made natively available be the cloud vendor to ensure the vendor version is not proprietary causing a code adjustment causing unexpected delays in migration. These products provide DevSecOps teams with the freedom to develop and deploy cloud-native applications using the languages, tools, frameworks and infrastructure that best meet their needs.

- **Sustainability –** The transition to the cloud enables us to consolidate our data centers and avoid on-premises deployments at disparate sites. To take optimal advantage of these sustainability gains, work closely with cloud partners that offer data transparency, drive renewable energy adoption, improve water efficiency and attain environmental certifications. These considerations should be part of any selection process.

- **Adjust Acquisition Strategies –** Acquisitions must include cloud-smart principles, common shared services and Agile software development methodologies. Cloud acquisitions should leverage a service-enabled architecture with automation of tasks and processes that limit human input and error across infrastructure, configuration, software and testing. Strategies must include clear roles and responsibilities, performance metrics, service level agreements and costs transparencies.

With your cloud acquisition complete, the next steps to ensure successful deployment and implementation include:

- **Establish Cloud Governance –** Establishing a governance structure for cloud management is foundational to operational sustainment. The structure should include dedicated management roles and responsibilities as well as advisory and decision-making bodies to assist in resolving architectural issues. Successful governance will take advantage of cloud automation to eliminate the need for manual oversight and repeated issues of the same form. Consider creating an Enterprise Cloud Management organization that can establish onboarding processes, monitor service usage, adhere to architectural standards established by the governance body, oversee risk management and compliance as well as provide financial management. Effective governance will ensure that you will be able to take advantage of the continuous innovation occurring within the cloud ecosystem.

- **Develop and Execute a Cloud Talent Management Plan –** Developing and executing a talent management plan is an essential component required for multi-disciplinary teams of cloud professionals. Implementation of a talent management plan will enable those closest to the needs and challenges to impact those fields relevant digital innovation specialties. Cloud design education is necessary to ensure that the existing workforce is equipped to enact the necessary paradigm shift.

- **Build a Secure Cloud Architecture –** A well-defined and well-constructed cloud-based architecture is a critical mission enabler. The architecture should focus on enabling mission criticality, data integrity, operational resilience and availability in a secure environment. A secure cloud architecture that reduces technical debt and duplication of effort will result in successfully delivering common shared services, data management services and cloud-native software development services.

Cloud computing is an opportunity for government to build on the benefits that consumers and businesses have realized from cloud computing to deploy new technologies with the goal of significantly improving the efficiency of governmental operations and the public services it offers.

Cloud Buyers Guide References:

The Cloud First Policy (2010) was intended to accelerate the pace at which the Federal Government realized the value of cloud computing by requiring agencies to evaluate safe, secure, cloud computing options before making any new investments.

The Federal Risk and Authorization Management Program (FedRAMP) (2011) was established to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government. FedRAMP empowers agencies to use modern cloud technologies, with an emphasis on security and protection of federal information.

The Cloud Smart Strategy (2018) is the second release from the Office of Management and Budget (OMB) following the first OMB release titled Cloud First in 2011 that was a part of the Federal Government IT Modernization effort. The Cloud First initiative stated that the Federal Government had to move to the Cloud but did not provide specific guidance how to accomplish cloud adoption. The Cloud Smart strategy provides more guidance surrounding security, procurement, and necessary workforce skills to foster cloud adoption and implementation.

The State Risk and Authorization Management Program (StateRAMP) (2021) represents the shared interests of state and local governments, third party assessment organizations, and service providers with IaaS, SaaS, and PaaS solutions. StateRAMP is built on the National Institute of Standards and Technology Special Publication 800-53 Rev. 4 framework, modeled in part after FedRAMP, and based on a “complete once, use many” concept that saves time and reduces costs for both service providers and governments. Like FedRAMP, StateRAMP relies on FedRAMP Authorized 3PAOs to conduct assessments.

CompTIA Worldwide Headquarters
CompTIA Member Services, LLC
3500 Lacey Road, Suite 100
Downers Grove, Illinois 60515

630.678.8300

CompTIA.org