HYBRID IT: EMPOWERING TODAY’S DIGITAL GOVERNMENT WORKER

Best Practices for Building a ‘People Critical’ Organization

A Digital Government Series by Unisys Corporation
TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Building Hybrid IT with Secure, Unified Management</td>
<td>4</td>
</tr>
<tr>
<td>Securing Servers in the Public Cloud with Unisys Stealth</td>
<td>6</td>
</tr>
<tr>
<td>Proactively Managing SLAS with Unisys VantagePoint</td>
<td>7</td>
</tr>
<tr>
<td>Real-Time Dashboard</td>
<td>7</td>
</tr>
<tr>
<td>Conclusion</td>
<td>8</td>
</tr>
<tr>
<td>About Unisys</td>
<td>8</td>
</tr>
</tbody>
</table>
INTRODUCTION

When the White House launched the federal Cloud First strategy more than five years ago, agencies moved cautiously to adopt cloud models. Many expressed a preference for keeping data and applications in private clouds, citing security and management concerns. Those that adopted public clouds often focused on gaining efficiencies—for example, by moving e-mail services, public-facing web pages, and storage into off-premises clouds. However, over time, agencies have gained greater confidence in their ability to manage and secure their cloud environments, and so many now are looking beyond mere cost savings to the improved agility and innovation that comes from a robust cloud environment. Agencies are moving more and more data and applications to the cloud.

As their cloud environments mature, agencies can expect to operate hybrid IT infrastructures that leverage a mix of on-premises, private-cloud services and third-party, public-cloud services. In fact, most government IT environments today are being architected using hybrid cloud configurations, providing services such as email, compute, and storage, while efficiently delivering mission-critical applications and citizen services. Ideally, the hybrid IT environment enables agencies to deploy applications using the IT infrastructure that best fits their mission needs in terms of cost, flexibility, and speed of deployment.

However, transitioning to a well-managed hybrid cloud environment can pose a number of challenges. Many organizations have encountered difficulties creating a unified management structure that ensures the most cost-effective deployment of resources. Similarly, some organizations have struggled to create interoperability among diverse internal and external IT assets. Managing service-level agreements with third-party cloud providers can also prove problematic. Perhaps the most difficult challenge is maintaining the high levels of security required of government organizations.

Federal Cloud Adoption Grows

Federal agencies are rapidly expanding cloud deployments, according to research firm IDC, which says the administration’s fiscal year 2017 budget increases cloud spending by 70 percent over 2016.

“We believe that cloud spending will eventually grow to about 50 percent of all government IT spending, but that number will not be reached until 2018,” said Shawn McCarthy, research director for IDC Government Insights, in a February 10, 2016, press release.

None of these issues is insurmountable, but in order to achieve the promised gains of cloud computing, agencies should consider six key areas as they embark on their journeys to hybrid IT:

1. Cloud services and deployment models
2. Resiliency
3. Interoperability
4. Security
5. Service Level Agreements
6. Governance and Cloud Service Management

The successful transition to a hybrid IT environment is an essential building block of a digital government organization that leverages data analytics, virtualization, cloud, mobility, and other emerging technologies to meet expanding mission requirements, even as budgets tighten. A digital organization equips its employees with advanced applications and access to data to carry out their mission responsibilities, while also delivering to citizens the information and services they need anytime, anywhere, and on multiple devices.
BUILDING HYBRID IT WITH SECURE, UNIFIED MANAGEMENT

The journey to hybrid IT starts with a deep understanding of your employees’ unique roles and responsibilities in supporting your agency’s mission and objectives. What are their working patterns, how do they use technology in their day-to-day activities, and what computing needs do they have? This information is critical for aligning the right devices, applications, network, storage, and support with specific roles and needs. And because roles change and requirements evolve over time, it’s essential that an organization analyze, evaluate, and optimize IT systems regularly, so it can deliver continuous alignment between the computing environment and the end user. This laser-like focus on end-user requirements provides the foundation for successfully addressing the six key areas for hybrid IT.

1. Cloud Services and Deployment Models

As agencies transition to hybrid IT, they have a number of cloud service and deployment options available. For example, some infrastructure will be deployed as platform-as-a-service (PaaS) cloud platforms. In addition, some IT assets will be deployed as infrastructure-as-a-service (IaaS) or software-as-a-service (SaaS), while other assets will continue to perform in more traditional roles as either general-purpose or specialized functions. These examples illustrate some of the possibilities:

- **IaaS**—provides servers, storage and backup, and network as virtual items in a cloud service. The consumer manages these components and often must provide, or at least specify, the operating software for the servers.
- **PaaS**—provides a common virtualized platform services catalogue, such as unified communications, database services, development platforms, and virtual work services for end users.
- **SaaS**—is a common software infrastructure provided through cloud infrastructure by license, typically for the number of users who will use the service. Typical SaaS services include cloud-based IT service management, cloud-based image management, and cloud-based email and collaboration tools.

Among their cloud options, agencies can use:

- **Public Clouds**. These offer highly elastic and practically infinite capacity available on demand with little or no long-term commitment, as well as hourly rates for server usage and discounts for clients that choose to commit to monthly, semiannual, or annual periods. Public cloud providers include Microsoft Azure, Amazon Web Services, Rackspace, Google, and IBM.
- **Private Clouds**. These can be on-premises or third-party hosted clouds designated solely for the use of a single customer. They can also be a shared private cloud or “community cloud,” which is a multi-tenant environment that logically separates infrastructure components for different clients.
- **Hybrid Clouds**. These bring public and private cloud infrastructures together into a unified service-delivery platform that can be managed and monitored from a single tool.

The first step in your journey to hybrid IT is gaining a clear understanding of your business requirements. What capabilities do your employees need to carry out their mission responsibilities?

The right cloud provider will rationalize an organization’s existing infrastructure with cloud services and deployment models and build a roadmap that brings data center, internal cloud, and external cloud resources into a flexible and agile unified fabric that ultimately aligns IT with strategic mission objectives.

The challenge facing government organizations is managing the complex mix of IaaS, PaaS, and SaaS services within their hybrid environment. To achieve the expected efficiency gains and other benefits of their hybrid environment, they need to match the right workloads with the best-fit cloud technology, while also orchestrating the deployment of applications and services across the enterprise.

**Simplifying Deployment of Cloud Services with Unisys VantagePoint.**

Unisys VantagePoint™ reduces management complexity to help agencies address these challenges and transition smoothly to a hybrid IT environment. VantagePoint is a multi-sourced business-services aggregator that improves enterprise performance, and lowers operating costs through a repeatable process model, and a single intuitive interface where access, visibility, and enhancements to business and mission services are personalized to the user’s needs.
VantagePoint provides:

- **Effortless Provisioning of Cloud Services**: VantagePoint includes public cloud provisioning capabilities that enable IT service managers and operations staff to take advantage of innovative trends and technological advances in the public cloud space. In addition, it offers an Enterprise Services Broker that seamlessly integrates with Unisys managed shared private cloud services in Unisys data centers or even private, dedicated cloud services.

- **Ease of Use and Multi-Device Support**: VantagePoint provides enterprise IT departments with the power of on-demand self-service. This allows IT to track and manage user enablement. It gives users the ability to provision resources, plus gain immediate access to the power of cloud computing. Through a multi-sourced retail-like Enterprise Services Catalog, users can provision Hybrid Cloud Services from anywhere, anytime, across any end-point device — helping IT meet expectations for ease of acquisition. What’s more, with this solution, the management of all supporting back-office integration services is completely invisible to agency personnel.

- **Integrated Tools That Accelerate ROI**: VantagePoint speeds time to value by combining a pre-built enterprise services catalog, an intuitive and flexible user interface, and powerful data integration and analysis capabilities. And it does it all within a SaaS solution that dramatically improves service delivery levels — in a matter of months, not years.

### 2. Resiliency

Cloud providers are vulnerable to the same disaster scenarios facing other data-center operations, so it’s imperative that as organizations move along their hybrid IT journey, they take into account resilient services, such as business continuity (BC) and related high availability (HA) and disaster recovery (DR) services.

A cloud provider should offer multiple tiers of resilient services that are defined by an organization’s mission imperatives and expressed as specific recovery time objectives (RTOs) and recovery point objectives (RPOs). For example, costs typically range from the most expensive (e.g., an RTO within minutes and fully automated, with an RPO of no data loss) down to the more reasonable (e.g., an RTO within 72 hours for manually implemented procedures, with an RPO of 24 to 36 hours based on nightly backups, etc.), depending on an organization’s BC requirements.

The highest cost for BC is reserved for infrastructure where lives might be lost during an RTO of hours or for agencies where the loss of data transactions could cost millions of dollars or disrupt critical citizen services. The right cloud provider will offer service options across each combination of RTO/RPO and provide pricing based on the gigabytes of data protected. This enables an organization to manage costs by associating value with data sets and discriminating between the levels of resiliency required for each of those sets.

### Additional considerations should include:

- Locations of resilient sites
- Transparent monitoring/management
- Annual testing
- Any unique support requirements

### Ensuring Continuous Operations with Flexible Unisys Business Continuity Offerings.

Unisys maintains data-center facilities in Eagan, Minnesota, and Salt Lake City, Utah, for shared and dedicated private cloud services. The Eagan facility can provide agencies with a secure private cloud. Unisys also has a strategic partnership with Microsoft Azure that includes access to four regional U.S. facilities in Virginia, California, Illinois, and Texas, with another being built in Iowa.

In addition, Unisys partners with data-center facility providers that are near Azure data centers so clients can house critical physical IT infrastructure, such as mainframes or proprietary UNIX servers, close enough to the Azure production like Windows and Linux Workloads infrastructure to avoid latency issues between applications.

Unisys provides the tools to integrate any cloud provider an organization might prefer. For example, Unisys can manage a large cloud service provider like IBM to offer a blend of IBM DR facilities in a location that will adequately support a company’s BC requirements.

### 3. Interoperability

One of the key tenets of a hybrid IT journey is the ability to build a unified IT infrastructure out of existing investments in legacy technologies and new investments in cloud platforms. However, legacy systems do not always integrate easily with systems built using modern technology. Therefore, any hybrid IT initiative must include a thorough evaluation of interoperability across all components that will comprise the new infrastructure.

There are three main ways to address interoperability:

- **With Legacy Systems**: The cloud provider should be able to create a virtual network that securely connects an organization’s legacy systems (including data and applications) to the scalable, on-demand infrastructure of a public cloud and enable movement of workloads as required.

- **With Other Cloud Systems**: The cloud provider should offer an automated service catalog that allows choice of approved cloud systems and an IT Service Management (ITSM) infrastructure that creates automation between the fulfillment of provisioning and the introduction of the new infrastructure into the ITSM monitoring and management tool suites. Also, selection of a new service component, such as a mission-critical server, should automatically create the additional supporting services, such as BC resources for the mission-critical server.
• With Overall IT Strategy: The cloud provider should offer cloud advisory services that can provide a roadmap for interoperability and transformation services focused on the specific cloud implementation an organization has chosen. This roadmap will allow a CIO to recommend areas to accelerate cloud-based implementations to support CFO strategies.

Evaluating, Planning, Migrating, and Managing Applications with Unisys Cloud Advisory Services.

Unisys Cloud Advisory Services provide organizations with a strategic view of their application environments that aids in building a roadmap to migrate workloads from existing, on-premises resources to a cloud-based platform in the most efficient manner possible. Specific services include:

- Business Analysis and IT Assessment: Audits the workloads to be managed and identifies the best migration approaches to the cloud.
- Workload Management Resource Planning: Includes the identification of existing or desired resources by skill set or technology platform.
- IaaS/PaaS/SaaS Right-sizing: Incorporates the IT assessment and plots a path to cloud IaaS, PaaS, and/or SaaS solutions.
- Cost/Benefit Analysis: Places a dollar value to the potential savings Unisys can provide by managing selected workloads in the cloud.

4. Security

The use of remote computing resources opens up new possibilities for security breaches, so it’s imperative that any organization on a hybrid IT journey expand its security strategy to account for the unique risks associated with cloud technologies. Agencies must also ensure that their hybrid IT environment complies with government’s stringent security requirements, such as the Federal Information Security Modernization Act (FISMA), Federal Information Processing Standards (FIPS), Federal Risk and Authorization Management Program (FedRAMP), Healthcare Insurance Portability and Accountability Act (HIPAA), and International Traffic in Arms Regulations (ITAR). The cloud provider should offer security services that include:

- Appliances that provide unprecedented server-level security for both cloud-based and internally supported server infrastructure.
- Agents that can be installed on IaaS server infrastructure to protect data and applications residing on public clouds.
- Encryption and decryption capabilities that are transparent to the operating system and to the applications running on it.
- The option to manage security keys on-premises or within the provider’s hosted solution.

SECURING SERVERS IN THE PUBLIC CLOUD WITH UNISYS STEALTH

Unisys Stealth® appliances offer unprecedented security. They create a secure communications tunnel, where the data is encrypted and split before transmission. In addition, Stealth cloaks endpoints from users or devices, except those who are pre-identified as part of a “secure community,” referred to as a Community of Interest (COI). Managing COIs is easy with Stealth, because access is defined by device or user identity, rather than physical topology.

With Stealth, organizations can:

- Encrypt data in the communication channel all the way through to the virtual server, rather than just to the cloud boundary.
- Cloak endpoints in the public cloud from other tenants in the cloud and from hackers attempting to infiltrate the cloud – even from the cloud providers’ own management consoles.
- Maintain control of protected assets, since the organization can manage encryption keys within its own data center.
- Leverage Microsoft Active Directory or other identity stores to enforce identity-based access to virtual servers in the public cloud for only selected users or devices – without requiring application or infrastructure changes.

5. Service Level Agreements

A key component of a people-critical hybrid IT infrastructure is providing the level of service that citizens demand and that government users need to do their jobs. The best way to ensure this is to specify and clearly document the level(s) of service required with agreed-upon SLAs.

Below is an example checklist of questions cloud providers should be able to answer:

- Does the cloud provider employ a service excellence team that analyzes incident data across all client accounts to drive innovation and improve service quality?
- Does it periodically review service demands to see if they have unexpectedly grown beyond the original service specification?
- Does it clearly specify who is responsible for which parts of the computing environment, so an organization knows the appropriate resource to contact when issues arise?
- Does it offer a self-service portal with dashboards that provide transparency into current service-delivery/fulfillment and drill-downs into specific issues?
- When choosing use of public cloud services, what financial penalties will the provider bear for missed SLAs?
Unisys VantagePoint integrates disparate data sources from across the enterprise and applies powerful analytics that generate insights in real time. Intelligence is personalized and delivered through distinct service views across people, operations, and mission. Instead of manually stitching together data from siloed services, users now view key performance indicators (KPIs), SLAs, and actionable insights through a single consolidated dashboard. This facilitates proactive, informed decisions that improve operational and mission performance and lower costs.

For example, the VantagePoint operations dashboard provides real-time information that organizations can use to proactively manage cloud service levels, including:

- Enterprise systems management (ESM) metrics
- Work queues
- Analytics and trending
- Service catalog
- Provisioning
- Operational knowledge

6. Governance and Cloud Service Management

Cloud services must be managed by a governing entity and guided by policy and governance as an essential consideration for organizations on a hybrid IT journey.

The main challenge facing internal IT organizations is how to adopt a governance model that will allow agency leaders to drive the adoption of new cloud service models and adapt quickly to changing operational and mission requirements. Organizations that succeed in taking advantage of the opportunities presented by public cloud services establish mature governance processes that make service automation a high priority.

To support the demands of agency leaders, cloud providers should offer deep levels of service transparency that allow them to drill down, in near real time, to the trends in current service delivery. Public cloud costs and flexibility have already shown that it is possible to build fully automated IT services with nearly infinite on-demand compute capacity to meet peak loads. This encourages agency leaders to demand more control over Service Governance, following the example of public cloud service governance. However, these same leaders often doubt whether the IT staff can reach the highest value points on the curve presented in the figure below.

Still, continuous improvement should be a baseline goal for organizations on a hybrid IT journey, and the right governance framework will help them maintain service levels as they climb the ladder toward the ideal “Everything-as-a-Service” destination.
CONCLUSION

The convergence of many forces – the consumerization of IT, the proliferation of mobile devices and social applications, increasing employee and citizen expectations for high-performance service – have changed the scope of mission-critical computing. As a result, government organizations are trading in their old, inflexible, exclusively on-premises data centers for hybrid IT infrastructures that bring the best of legacy systems and cloud services and platforms together into a unified fabric – one built expressly to meet the many and varied needs of today’s users. That’s what it means to be people-critical.

However, the journey to a people-critical hybrid IT environment can be an uncertain one, marked by concerns around interoperability, business continuity, security, governance, and more. This is why it is imperative to partner with a cloud provider that not only covers the technology portion of the equation, but also has the expertise, best practices, and proven solutions to address the entire spectrum of challenges the hybrid IT journey creates.

Once an organization fully embraces hybrid IT, it can realize powerful benefits across the board:

• For government workers, it makes the right technology and support available when and where they need it. This not only boosts their productivity but also empowers them to be drivers of innovation.
• For IT departments, it means greater visibility into the computing needs of users and citizens, increased speed and agility in meeting their demands, and the ability to make fiscally responsible decisions.
• For the agency, it brings a people-critical approach to IT that delivers cost savings through results-driven operations and productive staff who are focused on serving internal customers (i.e., government workers) and citizens.

Overall, government organizations will achieve increased efficiencies by lowering infrastructure costs, minimizing capital expenditures, better aligning costs with business utilization, and reducing manual labor. They also will accelerate service delivery by enabling self-service, automated provisioning, and proactive resource monitoring. And they will be able to respond more quickly to new mandates and initiatives by enhancing the IT department’s ability to configure new infrastructure and make a broader service catalog readily available to users.

THE UNISYS SERIES ON DIGITAL GOVERNMENT

Becoming a digital government organization

The transition to digital government is not an all-or-nothing proposition. Agencies will continue to optimize and leverage their legacy environments while they identify opportunities to implement new hosting models; strengthen data collection, integration, and analytics; and expand their digital capabilities throughout the enterprise. The hallmark of a digital organization is its ability to leverage free flowing information through an interconnected world.

The next step for government agencies is to build on their experimentation and initial deployments to create a digital government roadmap. The lessons learned from earlier programs will help agency leaders establish priorities and identify the benefits they want to achieve. This planning will also help them create the governance mechanisms to manage their digital programs and keep them moving forward.

Digital government organizations will enjoy many benefits. Agencies will realize cost savings and operational efficiencies to help them meet expanding mission requirements even as budgets tighten. And the ability to collect and analyze the enormous amounts of data will generate insights for improving the mission capabilities of warfighters, civilian employees and government systems. Overall, digital government will empower employees to bring forward the most advanced and innovative solutions for spending taxpayer dollars wisely, serving citizens, and performing governments’ many missions.

For more information on Digital Government visit: www.unisys.com/digital-government

ABOUT UNISYS

Unisys is a global information technology company that specializes in providing industry-focused solutions integrated with leading-edge security protocols to clients in the government, financial services and commercial markets. Unisys offerings include security solutions, advanced data analytics, cloud and infrastructure services, application services and application and server software. For more information, visit: www.unisys.com