Key Considerations When Migrating Workloads to Public Cloud

Insight

Table of contents

Overview

Public cloud services have become central to IT strategy. The potential cost savings and agility are simply too compelling to ignore. And, as more enterprises move to a hybrid IT environment and service providers continue to enhance their offerings, public cloud services will likely gain in popularity in the coming years.

It's tempting for many IT and business leaders to want to push their organizations into the public cloud as quickly as possible to reap the benefits — to leap before they look. But taking the time to do necessary groundwork is important.

Why preparations are worthwhile:

- To be more resource-efficient (i.e. less time and money wasted)
- To mitigate and minimize risks
- To prevent reactionary moves and fire drills later on

A better approach to public cloud

Insight SVP and GM, Shawn O'Grady, shares how to be successful with public cloud adoption.

76%
of IT leaders are **more cautious now**
than they were one year ago

PART 1

Empirical findings

In September 2017, Insight commissioned IDG Research to conduct a survey of 142 IT professionals about IT transformation. The results clarify the central obstacles and opportunities for IT leaders today — particularly when it comes to public cloud deployment.

#1: More than half (52%) of surveyed IT leaders said their organizations had moved one or more workloads away from the public cloud to an on-premises model.

#2: Reasons for repatriation included concerns about control over resources or data; pressure to meet regulatory compliance requirements; security concerns; lack of monitoring capabilities; and high costs.

#3: 76% of IT leaders are more cautious now than they were one year ago when considering public cloud adoption.

The important thing to understand is: Retrenchment doesn't need to happen. It runs counterintuitive to today's typical IT strategy to leverage the cloud for cost savings and added agility.

This ebook offers guidelines for those considering moving workloads to public cloud. By following the best practices provided here, enterprises can increase the likelihood of a successful move to the public cloud that will result in greater long-term value for the organization.

PART 2

Business needs

Organizations need to know and identify the business drivers, needs, goals, and risks to using and not using the cloud. That means:

Asking why the organization is considering moving particular workloads to the cloud

Determining the business stakeholders, governance, and technology

Identifying key operational details, as well as how they will be reviewed and validated to verify business needs are met

Having business stakeholder support throughout the process is critical. Obtaining buy-in from impacted parties like functional owners, end users, and supporting IT groups can make the difference between an unsuccessful and a successful project.

In addition, time should be spent assessing the true total cost of ownership by comparing costs of the current on-premises model vs. leveraging public cloud.

9 Common Mistakes to Avoid

Learn what not to do when migrating workloads in this whitepaper.

PART 3

Workload assessment

Armed with important background information and firm-level buy-in, IT leaders can continue by conducting a workload assessment. This will help the organization determine what should move to the cloud and what should remain on-premises.

First, it's important to understand that a workload is an application and the resources required to support the application, such as compute, network, and storage.

An example of a workload might be a three-tier application stack that includes:

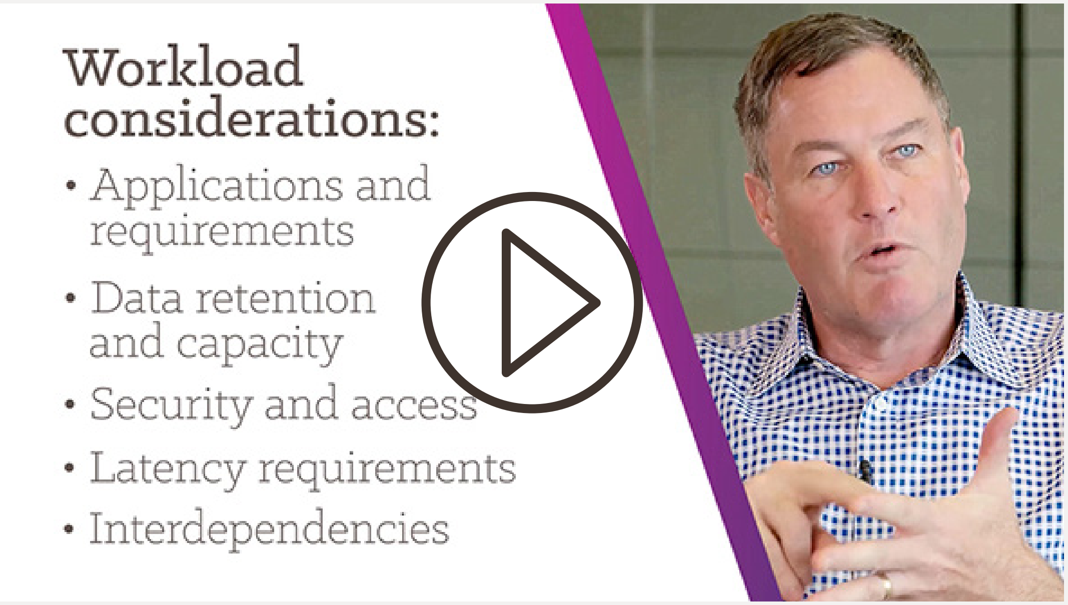
+ A web instance
+ A single database
+ A business application

These three components work together to perform a task. While the web instance and database might be on large servers hosting multiple web instances and databases, only the separate components are part of the workload.

Some helpful logic to identify what constitutes a workload would be: Can the components be separated or moved and still perform their basic task or functionality? If so, then most likely they are part of separate workloads. As an example, a single database can be moved to a separate database server, and thus the database server is not a workload but rather a platform that hosts workloads.

What is a workload?

Insight SVP and GM, Shawn O'Grady, offers an evolved definition of this key concept.

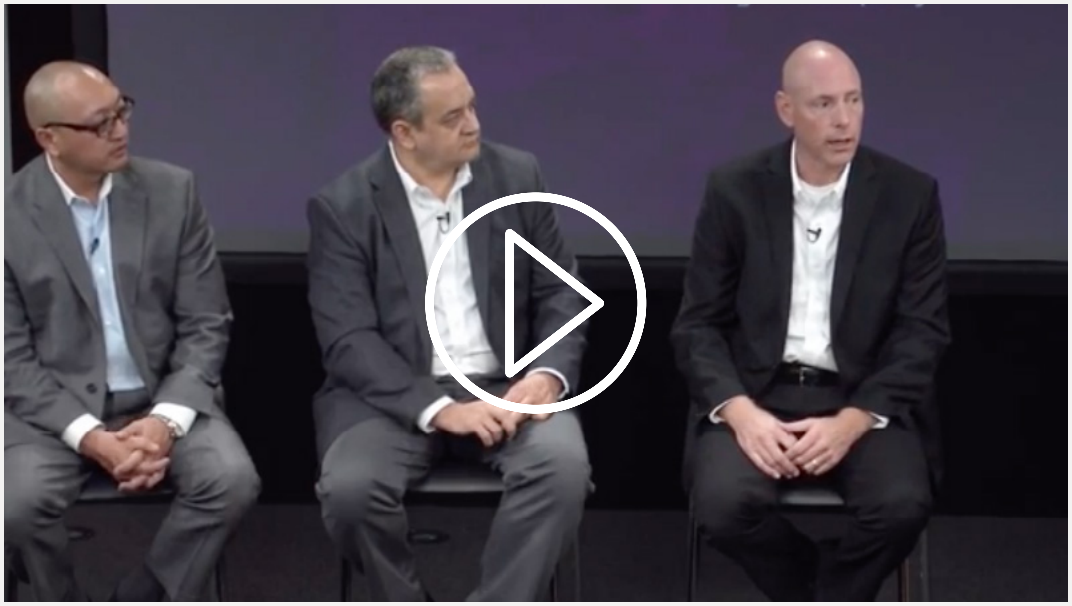


Workload considerations:

- Applications and requirements
- Data retention and capacity
- Security and access
- Latency requirements
- Interdependencies

How does Insight approach cloud platform workload alignment?

Insight National Portfolio Director of Consulting Services, Peter Kraatz, explains in this video.



PART 3

Workload assessment

Why do companies need to do these workload analyses? The fact is, many organizations are not aware of the number of applications they actually have. Because of this, they need to conduct an inventory and then assess the interdependencies of applications. Among the considerations are storage, networking, computing, backup, security, and total cost of ownership (TCO).

The results of workload assessments provide data to identify the most technically appropriate and cost-effective cloud platform to support a workload's business requirements. It's important because it can lead to benefits including time savings, reduced risk, reduced cost, and greater agility.

Workload assessment and alignment efforts drive best-fit platform decisions, as well as prompt next steps, including decommission, lift-and-shift, rearchitect, sustain, and re-platform.

Other critical steps include determining the cost variables; understanding the acceptance level within the organization of moving to the cloud; working from a defined and existing service catalog or portfolio; and understanding the service and how it is currently delivered.

PART 4

IT governance

In some ways, the shift to the cloud is a sea change much like the move to client-server computing was following the mainframe-centric days years ago. Without integrating cloud into IT governance processes, a company moving workloads to the cloud might see a decline in productivity and a rise in confusion among workers.

Getting cloud-ready

Management needs to ensure the organization's IT governance processes are cloud-ready. That includes making sure all necessary provisions are in place for systems and data security, privacy, and reliability.

While these areas have no doubt all been high priorities for on-premises IT, accounting for them in the public cloud is another matter — and expanding or amending the existing governance strategy is important.

Who's in charge?

In some instances, IT governance processes that have been conducted a certain way for years or decades will need to be altered, and it requires strong leadership skills to make sure services are not interrupted or degraded during the transition.

Companies need to determine who is responsible for managing the new environment, which might consist of multiple cloud services as well as on-premises IT. Because so many cloud initiatives are driven by the business side, line-of-business leaders will need to work closely with IT and operations executives to ensure a cohesive changeover to the new ways of doing things.

Good management also means understanding who is responsible for what when it comes to different aspects of IT and the cloud. This can vary depending on the type of cloud service.

Pro tip:

The benefits for migrating workloads to cloud must outweigh the costs and risks of doing so.

Organizations must always consider: How the choice affects their business, if the workload is ready for the cloud, and whether the business is ready to consume the workload in the cloud.

PART 4

IT governance

Questions of ownership

Identifying ownership can be challenging, particularly in new environments. For example, with Infrastructure as a Service (IaaS) and Platform as a Service (PaaS), internal IT is typically responsible for applications and data, but with Application as a Service (AaaS) that responsibility lies with the service provider. As a rule, service providers are responsible for operating systems, virtualization, servers, storage, and networking — regardless of the type of service. Data is the responsibility of internal IT.

Recent research shows that many organizations have misconceptions when it comes to management responsibilities. A 2017 report by research firm Vanson Bourne and data management provider Veritas showed that:

+ 69% of 1,200 global business and IT decision makers wrongfully think their organization's cloud service provider handles all data privacy, regulatory compliance, and data protection responsibilities.

+ A large majority of the survey respondents that use or plan to use IaaS offerings (83%) think their organization's cloud providers will protect their workloads and data against outages.

+ 54% think it's the responsibility of the service provider to securely transfer data between on-premises systems and the cloud. And, about half think cloud service providers are responsible for backing up workloads in the cloud.

Cloud service type	Administration	Applications	Data	Runtime	Middleware	O/S	Virtualization	Servers	Storage	Networking
Infrastructure as a Service	✓	✓	✓	✓	✓	—	—	—	—	—
Platform as a Service	✓	✓	✓	—	—	—	—	—	—	—
Application as a Service	✓	—	—	—	—	—	—	—	—	—

✓ Internal IT responsible — Service provider responsible

More on security

Many IT decision makers are unclear about cloud security ownership and how this might change with different service types. Unfounded assumptions can lead to unintentional outcomes like data breaches and vulnerabilities. Check out this whitepaper to learn more.

Insight

Moving Workloads to the Public Cloud? Don't Forget About Security

Key considerations for developing a cloud-ready cybersecurity strategy

Introduction

PART 5

Cloud provider evaluation

The overall assessment process should also include a comprehensive evaluation of cloud providers prior to making a selection. In some cases, organizations will need multiple public cloud providers based on workload requirements. But the object of the evaluation is to find the best platform and provider for a given workload.

Some of the criteria to consider include:

- Overall costs of the services
- The level of support offered by the vendor
- Provider experience in specific industries
- Regional or international coverage
- The economic status of the provider

PART 5

Cloud provider evaluation

Among the most important considerations are the security, privacy, and availability/reliability capabilities of the service provider. Good questions to ask are:

+ What sort of authentication and authorization platforms does the provider offer?

+ Do they offer information protection?

+ What type of encryption technology does the provider use and what is encrypted?

+ What kind of firewalls do they use to protect infrastructure?

+ Which directory services platform do they have?

+ What compliance provisions does the provider have in place?

Pro tip:

Companies need to align their business needs with the selection while also considering challenges that might be posed by using that particular provider.

It's important to understand that one provider might not meet all the needs of the organization. Enterprises also need to note that not all regions within a single provider offer the same services and capabilities.

PART 6

Third-party support

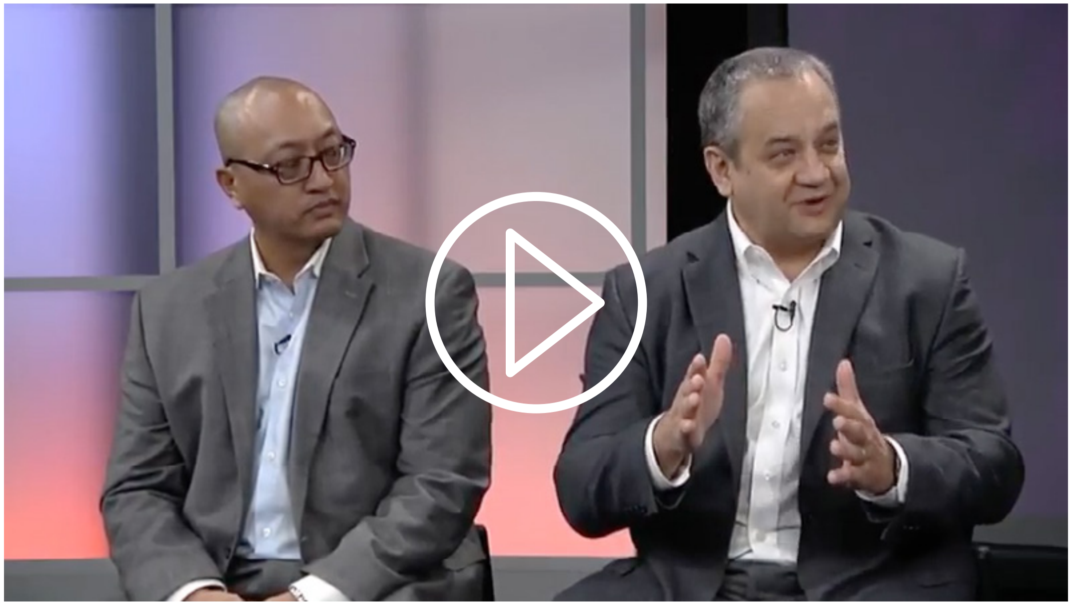
Once the assessment is complete and service providers have been selected — or even prior to the selection — it's vital to bring in the right partner to help with the migration process.

This partner must have an understanding of how to develop and execute a successful migration strategy, and have knowledge of all the technical components that will be impacted by a move to the public cloud. The partner can also help select the right tools and migration mechanisms.

Q: Why do organizations need help from outside?

A: Because in many cases companies do not possess the necessary expertise, experience, or time to migrate workloads to the cloud. There are many moving parts involved, and unless an organization has extensive experience dealing with cloud migrations the learning curve can be steep.

Transforming your data center can feel like trying to change the wheels on your car as you're barreling down the highway. Learn why in this video clip.



PART 6

Third-party support

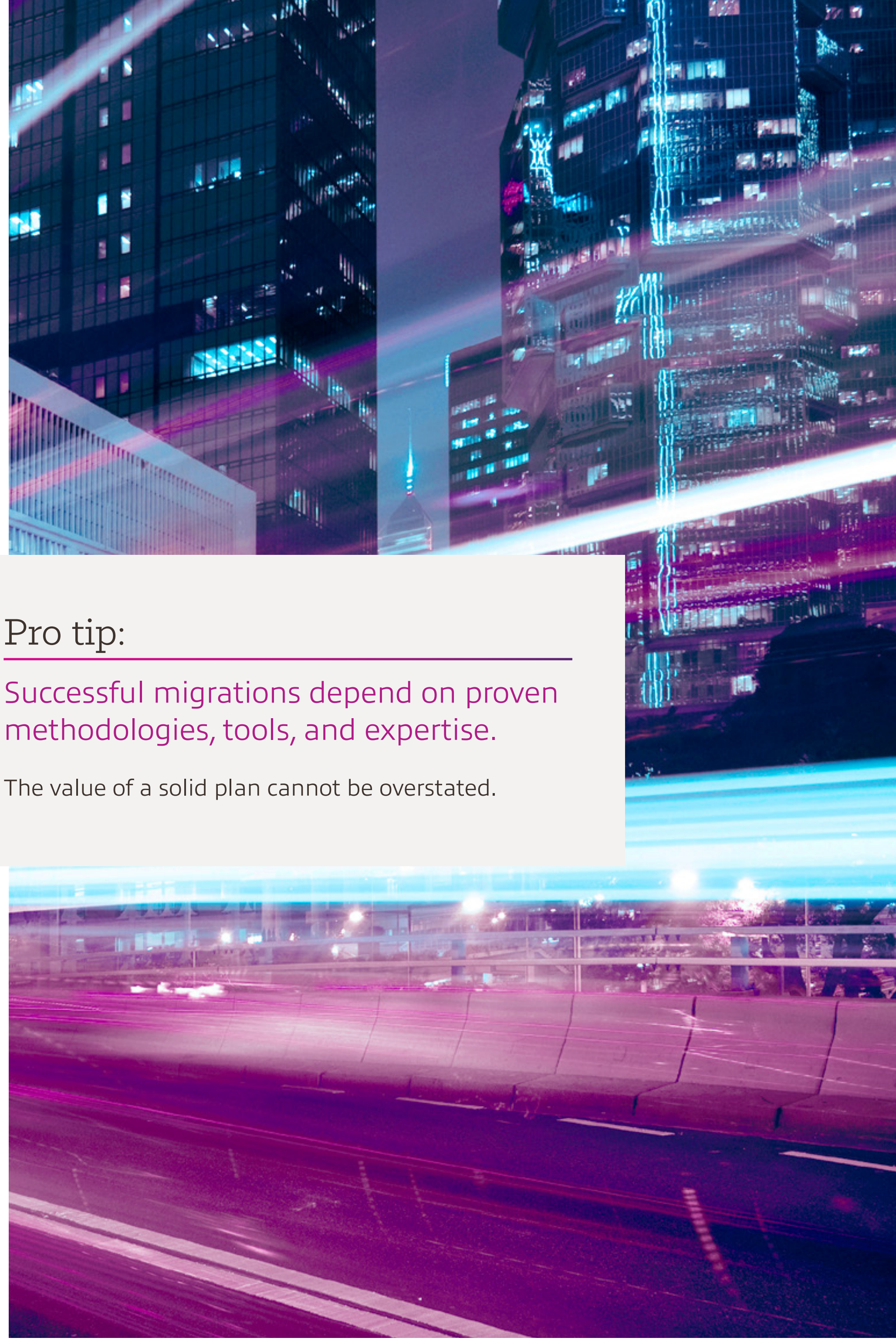
A pre-migration checklist

A company preparing to start a migration to the cloud needs to understand a host of variables, dynamics, and implications. These include:

+ The requirements of service level agreements (SLAs)
+ The security architecture that needs to be in place
+ Data access and flow issues
+ The migration paths required by different workloads
+ Data replication requirements
+ The financial impact as workloads are moved to the cloud
+ Managing the risk factors of the move to the cloud

Leveraging proven, migration methodologies are essential to minimize risk. Migration methodologies for assessing workloads, defining workload interdependencies, and combining workloads to move as a group are imperative to smooth migrations. In addition, methodologies for maintaining SLAs and conducting testing with all respective users are also critical to success.

There are many tools and migration mechanisms available, but finding the right ones to meet the organization’s specific needs can be difficult. Having a partner that understands use cases for tools can be a huge advantage.



Pro tip:

Successful migrations depend on proven methodologies, tools, and expertise.

The value of a solid plan cannot be overstated.

Conclusion

Moving workloads to the public cloud can be a significant and worthwhile endeavor for any type of business. But doing so without taking the necessary steps can lead to huge problems, including a lot of wasted time and money.

The number of companies that have brought workloads and applications back on-premises after initially moving into the cloud is a testament to the fact that not every workload is best suited for public cloud. It’s likely that some or even most of these companies did not perform a workload assessment prior to making the decision to migrate. Instead, they made a wholesale move into the cloud without giving thought to the impact of such a change.

Key takeaway

By conducting a workload assessment and adhering to other best practices, an organization can go a long way toward ensuring success with the public cloud as part of an overall move to a hybrid IT environment and a digital transformation.

solutions.insight.com | insight.com