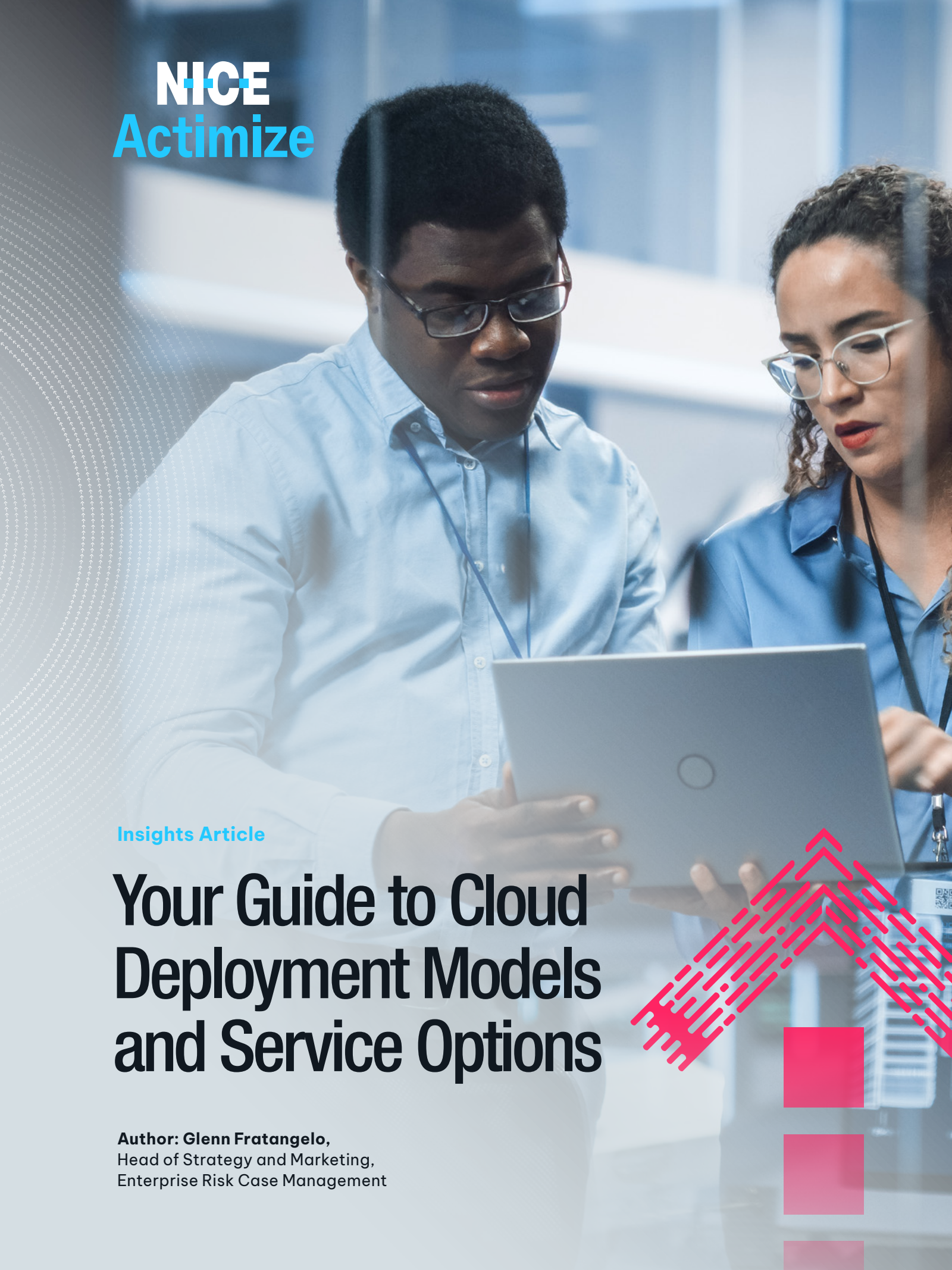
NICE Actimize



Insights Article

Your Guide to Cloud Deployment Models and Service Options

Author: Glenn Fratangelo,
Head of Strategy and Marketing,
Enterprise Risk Case Management

The key technology that transformed how organizations increased agility and scalability while reducing cost is cloud computing. But the heavily regulated financial services industry has lagged in cloud adoption. Why? Concerns around security, compliance, and the prospect of migrating massive quantities of sensitive data is a daunting undertaking.

There are other challenges. Many FIs are intimidated by the complexity and expense of transforming their legacy systems and applications when modernizing for AI and data, especially on a global scale While modernization has a price, it's benefits can't be denied. Cloud providers that have continuously modernize systems and processes have made major strides in strengthening security and compliance offerings. This trend of moving to cloud is growing, as financial institutions (FIs) understand cloud migration is a necessary step to keep pace with digital transformation.

Risk-averse mindsets are being replaced by competitive drive to maintain an edge against emerging cloud-native players with disruptive business models. These disruptors include fintechs and non-traditional payment services providers. Consequently, it's no surprise that research indicates that 8 out of 10 bank executives are either already or planning to migrate the majority of workloads to the cloud.[1]

In this article, we'll explore cloud deployment models, service options, and the impact of different cloud-deployment scenarios.

Cloud Deployment Models

Cloud adoption models differ across the industry. Cloud covers a broad range of use cases. It supports the technology needed for AI and machine learning, improves operational resilience, enables real-time fraud detection and prevention, and accelerates development and delivery of cutting-edge digital products and services.

Public Cloud

Public cloud involves using cloud infrastructure provided by third-party service providers to host applications and store data. The cloud provider owns and manages the hardware, software, and networking. This enables organizations to benefit from the cloud's scalability and flexibility—without investing in and managing their own infrastructure. FIs can cherry pick the services that best fit their needs and easily experiment with new technologies.

There are cost efficiencies to public cloud: Organizations can pay for what they use on a subscription or pay-as-you-go basis. This helps reduce costs associated with purchasing and maintaining on-premises infrastructure. Public cloud also offers robust disaster recovery capabilities, which is critical to mitigating data loss or system downtime that can arise from, say, climate-induced events.

Private Cloud

Private cloud refers to a type of cloud computing environment where the computing resources, such as servers, storage and networking equipment, are dedicated solely to a single organization. Depending on an organization's needs, the cloud infrastructure can be managed and hosted on-premises or in a third-party data center.

Private cloud has distinct advantages over public cloud. Unlike public cloud infrastructure, which is shared between multiple users or organizations, private cloud offers increased security, control and customization options. Some examples are encryption, firewalls and intrusion prevention systems. Entities that demand high levels of performance and security, like government agencies, healthcare providers and financial institutions often use private cloud for these reasons.

Many software as a service (SaaS) providers use a virtual private cloud (VPC) model where a secure, isolated private cloud is hosted within a public cloud. VPC customers can run code, store data, host websites, and do anything else they could do in an ordinary private cloud, but the private cloud is hosted remotely by a public cloud provider.

Community Cloud

Community cloud involves a shared cloud computing environment between a group of organizations with similar interests or requirements. Like public cloud, the infrastructure is hosted by a third-party provider and accessed via the internet, but it's designed for a specific community of users, for example, educational institutions.

This approach can offer cost savings and resource pooling, because the services and infrastructure are shared among multiple organizations. It also provides greater customization and security than a public cloud since its purpose-designed for the community's needs.

Hybrid Cloud

Hybrid cloud combines the utility of public and private cloud infrastructure via a virtual private network (VPN) or direct connect. This enables data and applications to seamlessly move between the two environments as needed, enabling organizations to balance performance, cost and security requirements. For example, organizations might use the public cloud for non-sensitive workloads, like testing and development, while keeping critical applications and data in a private cloud environment.

This approach is popular in finance industries where sensitive data must be protected but there's interest in having the agility and cost savings of public cloud. Organizations also opt for this approach to avoid vendor lock-in and reduce the risks of relying on a single cloud provider, like downtime or data loss.

Industry Cloud

Industry cloud provides an environment that's designed for a particular industry, like finance or manufacturing. It offers specialized services, applications, and infrastructure tailored to vertical industry requirements via a complete product experience. This model also accommodates a composable approach, or the ability to dynamically allocate and reallocate resources, for more flexibility. Typically hosted by a third-party provider, this model can provide significant customization as it's built for industry needs.

Cloud Service Models

As FIs plan their cloud migration approach, they often assume that they need to simply lift and shift all their applications to infrastructure as a service (IaaS). But this can make it technically challenging to derive value from cloud-native offerings and ensure applications meet all business needs.

Ultimately, FIs must understand all cloud service options and evaluate the suitability of each approach in relation to their business priorities:

Software as a Service (SaaS)

SaaS involves software applications that are hosted by a cloud provider; users pay for access to the software on a subscription basis rather than purchasing and installing the software on their own infrastructure. The cloud provider manages the underlying infrastructure, like servers and databases, and manages the software application.

SaaS application usage can be quickly scaled up or down as needs change, enabling organizations to avoid over-provisioning and wasted spend. FIs often leverage SaaS as a scalable, cost-effective way to access applications while minimizing the burden of maintenance and upgrades, improving efficiency and enabling them to focus on core business functions.

Platform as a Service (PaaS)

PaaS enables organizations to lease any required cloud infrastructure for the entire application life cycle. The cloud provider manages the infrastructure and users are responsible for building and deploying their own applications; organizations can choose the tools, programming languages and frameworks that best meet their needs.

Many FIs use PaaS to build, test and deploy new applications without worrying about the underlying infrastructure, bringing new products and services to market more quickly. PaaS can also make it easier to predict costs and reduce capital expenditures because it eliminates the need to invest in hardware and software licenses. PaaS providers also typically feature strong security measures to protect against data breaches and other threats.

Cloud Deployment & Service Model Scenarios

Each cloud deployment and service model includes benefits and drawbacks, which has significant implications for an FI's evolving risk management and modernization programs.

For example, a large FI wants to improve its risk management by migrating to private, public or hybrid cloud. The FI is currently using on-premises infrastructure to manage its applications and data but understands that transitioning to the cloud could optimize its security and compliance position. What are the benefits of each model?

Cloud Deployment Scenarios

Private cloud:

- Enforce its own security policies
- Avoid potential performance and latency issues
- Customization could support security measures
- Greater visibility

Public cloud:

- More expertise to devote to security
- Standardized services
- Improved cost effectiveness
- Flexibility could improve responsiveness

Hybrid cloud:

- Improved data management and governance
- Agile infrastructure
- Maintain availability and accessibility of critical applications

Service Model Scenarios

PaaS:

- Supports specific application requirements that can't be met with off-the-shelf software
- Full control over the development process and ability to tailor applications to exact requirements
- Requires ongoing resources and IT expertise for application maintenance
- Requires initial investment in development resources, hardware, and software licenses
- May offer greater control over data security
- Facilitates collaboration among different teams and departments within the organization, helping improve risk management efforts

SaaS:

- Supports rapid deployment and scaling of applications, reducing the time and resources allocated to application maintenance and upgrades
- Accelerates implementation of standardized applications
- Typically designed for specific risk management needs
- Long-term cost effectiveness due to the subscription fee model
- Vendor handles all maintenance and upgrades, minimizing the need for in-house IT expertise
- Services and users can be added or removed as necessary
- Accessible from anywhere, which can streamline risk management collaboration efforts for remote workers

The right cloud migration approach can make a drastic difference in an organization's modernization journey, as can an experienced cloud partner. When determining which cloud deployment and service model is appropriate, organizations must consider several factors, including their existing IT infrastructure, data security and regulatory requirements, the level of control and customization needed, the scalability of the solution, the potential for cost savings, and the ease of integration with

For more information about cloud-based NICE Actimize solutions, go here.

---

[1]Banerjee, P. (2022, September 22). Forecast for the banking industry: nearly 100% chance of cloud. www.forbes.com https://www.forbes.com/sites/forbesfinancecouncil/2022/09/22/forecast-for-the-banking-industry-nearly-100-chance-of-cloud/?sh=7db7de246062

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance.

The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

www.niceactimize.com