Cutting through the fog:

Key considerations for migrating payments to the cloud

CGI

Realizing the full potential of the cloud—whether private or public—is enticing for banks but often is a very complex process.

CGI All Payments has helped many banks work through that complexity, address risks and deliver highly resilient, available solutions for payment processing.

Introduction

The arguments for why banks should consider replacing their data centers with the cloud are compelling. The potential benefits include sustainability, resource elasticity, reduced capacity planning, improved resiliency, increased efficiencies and lower costs.

These many stated benefits are why, of the 311 banking executives we interviewed as part of our 2024 CGI Voice of Our Clients program, 61% are planning to migrate at least 20% of their core business applications to the cloud over the next two years.

While many banks view the private cloud as less of a security risk, most banks have hesitated to move their core systems to the public cloud because of its unique security challenges. Security is of primary importance for banks as they deal with data sets comprising almost 100% personally identifiable information (PII), and the regulatory and reputational impacts of any compromise are high. And yet, over 84% of CGI clients use cloud-based solutions, such as CGI All Payments, with a lower risk profile than their previous infrastructure.

Protecting core assets is one of many concerns banks face when moving to the public cloud. There also are legal security and regulatory requirements to consider.

It is clear that unleashing the rewards of moving your payments to the public cloud is challenging and can seem potentially overwhelming, which is why we aim to make it easier.

At CGI, we have a long history of helping clients successfully navigate complex projects—from securely steering satellites and delivering valuable defense data to processing passports and implementing market-leading payment systems.

Our latest payment deployments have involved private and public cloud as well as hybrid models, and three fundamental capabilities have helped our clients break free of the obstacles holding others back:

1 **Platform**
A fit-for-purpose, multi-cloud-native and cloud-independent payments platform.

2 **Experience**
Extensive infrastructure and application management experience.

3 **Security and Resiliency**
Advanced cloud security coupled with a robust risk management approach.

By combining these three capabilities, our clients have moved their payments to the public cloud securely and seamlessly, realizing the true promise of cloud infrastructure.

The right platform

Deploying applications to the public cloud presents a significant challenge: ensuring the entire technology stack will enable efficient and secure implementation.

Although migrating mainframe applications to the cloud is technically feasible, this approach is generally avoided. Mainframe applications are neither cloud-native nor designed to leverage cloud benefits, making such migrations impractical and potentially counterproductive.

When you consider moving your payments infrastructure to the public cloud, the first step is to find the right platform. This fit-for-purpose, multi-cloud-native, scalable and cloud-independent solution will make the most of the benefits of cloud deployment. Independence is a significant component in reducing cloud risk. While cloud providers have endeavored to make deployment more accessible by providing cloud-native tools, using these prevents the deployed solution's interoperability. It can also tie a bank to a specific cloud platform and generate inherent technology debt (i.e., the implied costs of updating less than optimal technology), which is why we partner globally with all of the major hyper scalers alongside cloud tooling.

Ahead of deploying our first client to the public cloud in 2019, we reimagined and engineered our payments platform, CGI All Payments, to meet these requirements precisely. Based on an ISO 20022 data structure, the platform is purpose-built for orchestration, real-time processing and certified network gateways. It also supports the 24/7 processing of any payment type.

Designing CGI All Payments to deliver these future-proof capabilities has enabled us to deliver public and private cloud deployments for more than five years and ensure our clients benefit from the resource elasticity, resiliency, high availability and other cloud benefits they need.

This has become hugely important as payment processing undergoes significant changes globally. Within the following year, nearly every bank around the world will need to support ISO 20022-based payments as all infrastructures migrate to ISO 20022. Domestic, regional and cross-border real-time payments running 24/7 are already a reality for some, and banks are beginning to recognize the business need to prepare accordingly. In addition, and highlighted further by the global pandemic, payments infrastructure needs to be more flexible than mainframes, with secure remote deployment and maintenance a must-have.

The right experience

Although finding the right platform to achieve the benefits of public cloud deployment is essential, without the right experience for deploying securely and within a resilient, self-healing cloud environment, your platform will fall short.

Proven cloud expertise and processes coupled with effective cloud risk management are just as critical for minimizing risks, costs and business disruption as choosing the right platform and payment solution.

On the guidance side

Before any public cloud deployment, we conduct an in-depth requirements analysis (CGI Cloud Risk Assessment), identifying the migration's why, what, when and how. This analysis facilitates proactive issue resolution, drives efficiencies and reduces risk. Success at this stage requires open and clear communication about requirements, issues, opportunities, feasibilities, etc. A trusted relationship based on honesty and close collaboration is a vital part of this.

On the process side

We have developed robust cloud processes and made a significant investment in staff training and certification to assist banks with process implementation. We train teams on how the deployed platform works, how to monitor it proactively and how to troubleshoot and handle issues—or run it on their behalf. These management processes are rigorously tested and, once operational, highly effective.

We were the first Scaled agile (SAFe) global transformation partner, and this approach to development and delivery has enabled us to reduce time-to-market while improving quality.

Our agile teams use multiple environments to develop code (e.g., non-production, testing, pre-production, production), enabling them to deploy less code per release and test more quickly and effectively. Additionally, through automated testing, the teams can ensure that required changes have no negative impact on code that is already working.

We deploy applications into truly fit-for-purpose environments, leveraging public cloud features such as automated patching and Kubernetes' self-healing to ensure 24/7 processing and high availability far beyond that of more traditional deployments.

While cloud resiliency makes failover less likely, process automation dramatically reduces geo-location failure recovery time to less than 30 minutes. All of this is pulled together by decades of experience in providing application managed services (AMS) to clients around the world. We deliver services under "least access" protocols by security-cleared staff with transparent service-level agreements, strong but simple governance processes and highly effective change management. These measures ensure high efficiency, low cost and high quality. All of our services are also well documented and auditable, which addresses one of the chief concerns of banking regulators when assessing the external service arrangements of banks.

The right security and resiliency

Security and resiliency are already a critical need for any payments infrastructure because they could potentially devastate an economy in case of a breach or major failure.

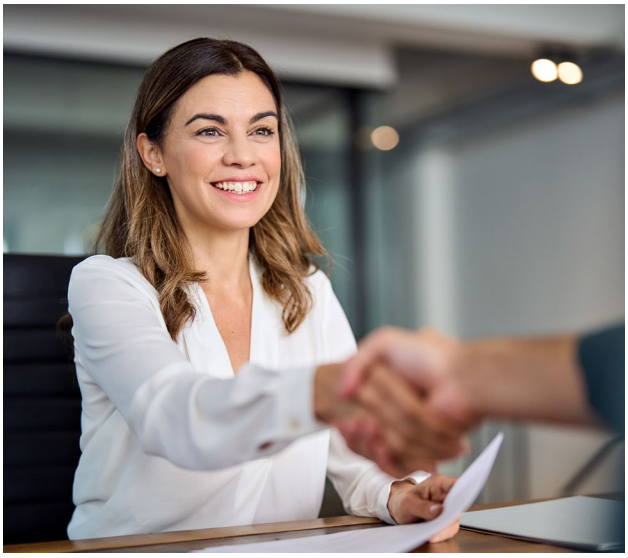
However, when processing moves to the public cloud and contains PII and payment data, another layer of scrutiny is involved. As with all technology introduction, if institutional understanding of real and perceived risks is low, not only are regulators concerned, but those responsible for security and resiliency within a bank often view this as a significant risk despite the obvious returns and improved controls that they will have in reality.

Although the primary public cloud providers—such as Microsoft Azure, Amazon Web Services and Google Cloud Platform—have poured significant investments into security and resiliency, hardening a specific environment falls to the organization responsible for the deployment. Cloud security controls must be set up and used correctly to ensure strong security and prevent the opening of doors that invite vulnerabilities using the proper security controls.

Likewise, data and application resiliency are critical in securing the availability of payment systems, and knowledge of how to get the best from them is paramount.

From a security perspective, it is essential to leverage multiple security tools that will automatically scan all layers, analyze source code, search for known third-party product vulnerabilities and validate runtime environment configuration. This helps minimize the ongoing risk of introducing new vulnerabilities through code changes, environment configuration and third-party software. Our overall security approach maintains a healthy balance between security risks, the impact of security controls on productivity and the costs of managing them.

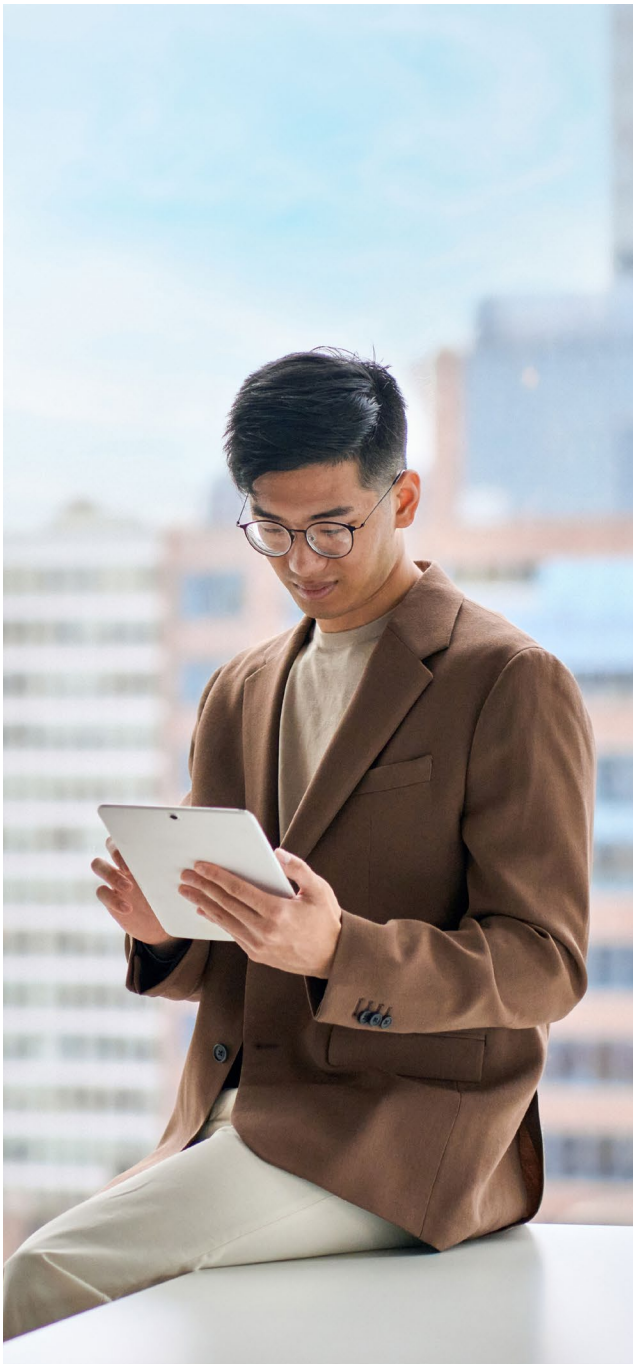
Attack tree threat modeling (threat analysis), which identifies possible attack vectors, is needed for public cloud security. Attack tree threat modeling helps to address the following primary security concerns for banks:



Extended attack surface to forge a payment or leak customer data:

This type of attack can be carried out by bank staff with access to the bank's payments processing systems and the staff of the bank's cloud service provider to some degree. The most important security controls to prevent this include:

- **Multi-factor authentication** for all types of accesses (e.g., user, administrator)
- **Cryptography** to protect payment data on multiple levels (e.g., encryption-at-rest, encryption-in-transit, digital signatures)
- **Segregation** of staff duties
- Use of **continuously scanned** private container registries and **restricted Internet access** from runtime environments



Extended attack surface to cause service unavailability:

The most important security controls to prevent this are network lockdown, DDoS protection, throttling and limited access to essential users. Access can be limited through a private virtual network and/or a site-to-site VPN between all sites (e.g., cloud service provider and bank) in a hybrid cloud deployment. It also can be limited through jump servers, management servers and virtual desktop infrastructure (VDI) without any option to install software.

With this approach, security is baked in, not bolted on, so there is less chance of missing a vulnerability or inadvertently creating one.

We also recognize that security is not just about technology but also about processes and people. Implementing a comprehensive security approach with proven processes helps maintain and increase security awareness among people, reducing possible attack vectors.

From a resiliency perspective, we leverage the inherent power of cloud to move from the old active:active idea to self-healing:active:hot:warm – essentially ensuring that production rarely falters, that failovers necessitated by disaster can be done seamlessly and with ample redundancy to ensure rapid return to operations in cases of cybersecurity or tooling update failures. This model change, coupled with a strong security stance, completes the rationale for moving to the cloud by delivering resiliency beyond the capabilities of traditional infrastructures such as mainframe.

Bringing it all together

For more than five years, our payments clients have been processing payments using our regulatory-approved public cloud solution, CGI All Payments.

Working closely with our clients, we have solved complex cloud problems and set forward-looking banks on a pathway to sustainability, lower costs, higher security and better use of the resources at their command.

Our clients' successes result from combining the right components with the right expertise and negating potential risks. Further, our work has led to repeatable execution. In line with market-voiced trends illustrated by our Voice of Our Clients survey, we expect public cloud deployment of payments infrastructure to become standard in the next few years.

Now is a great time to consider working with CGI to benefit from a public or a private cloud deployment. We can help you gain the advantages of whichever cloud service you choose.

Visit CGI.com to learn more, or contact us at info@cgi.com. We welcome an opportunity to discuss your cloud migration strategy.

About CGI

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-focused to help accelerate returns on your investments. Across hundreds of locations worldwide, we provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

cgi.com